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

**易爻（ CY\_20221106\_2330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 | 易爻 |
| 版本 | CY\_20221106\_2330 |
| 包名 | gz.aas.calc2yi |
| 域名线索 | 5条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2024年9月18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 | gz.aas.calc2yi\_6500\_37280627.apk |
| 文件大小 | 35.55MB |
| MD5值 | e062f8f3837bd2cf7aa4766a880161d0 |
| SHA1值 | 97455aa886c1b83334ef85d413d90c6d7c5f2354 |
| SHA256值 | fdc9ed53c6ff4eae54774186655db995f6cd2066b7ee6201d3baf36603569d98 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 易爻 |
| 包名 | gz.aas.calc2yi |
| 主活动Activity | gz.aas.calc2yi.MainActivity |
| 安卓版本名称 | CY\_20221106\_2330 |
| 安卓版本 | 6500 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| fundingchoicesmessages.google.com | IP: 172.217.160.78  所属国家: United States of America  地区: California  城市: Mountain View |
| developer.android.com | IP: 172.217.160.110  所属国家: United States of America  地区: California  城市: Mountain View |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.w3.org | IP: 128.30.52.100  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| goo.gl | IP: 172.217.163.46  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://github.com/flutter/flutter/issues/2897).It | io/flutter/plugin/platform/j.java |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/d.java |
| https://goo.gl/J1sWQy | c/a/b/a/d/f/g0.java |
| https://fundingchoicesmessages.google.com/a/consent | c/a/b/a/d/e/j2.java |
| 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/73620. | lib/arm64-v8a/libflutter.so |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/x86\_64/libflutter.so |
| https://github.com/flutter/flutter/issues/73620. | lib/x86\_64/libflutter.so |
| http://www.w3.org/XML/1998/namespace | lib/x86\_64/libflutter.so |
| http://www.w3.org/2000/xmlns/ | lib/x86\_64/libflutter.so |
| http://www.w3.org/XML/1998/namespace | lib/armeabi-v7a/libflutter.so |
| http://www.w3.org/2000/xmlns/ | lib/armeabi-v7a/libflutter.so |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/armeabi-v7a/libflutter.so |
| https://github.com/flutter/flutter/issues/73620. | lib/armeabi-v7a/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**

## **5. 签名证书**

**APK is signed v1 signature: False v2 signature: True v3 signature: False Found 1 unique certificates Subject: OU=AAS, CN=JonathanYang Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2011-05-19 16:34:48+00:00 Valid To: 2036-05-12 16:34:48+00:00 Issuer: OU=AAS, CN=JonathanYang Serial Number: 0x4dd546a8 Hash Algorithm: sha1 md5: fd232a53a9f7ced150a7b082a9beb70a sha1: 51ec0f46272e439cb8d3aede65353e4a3cf635eb sha256: 83dc571622d1529ff00d621071b9c3f1f3ccb213cdf043f789a630d70be2bf1d sha512: 32ed753011988b328e6300ab7572bf27c64bfe58de7bf6967a1e529cbca4d4aeb9accd8585020f019cee3151109280b560f38a8cd098766ea8b8e377469a7e77 PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: cf6861765c3c806b5732c5b3bfd6ff3dbd9a029eb7893af3025cc6fb7ccc7b70**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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 |
| com.google.android.gms.permission.AD\_ID | 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 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |

## **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。**