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

**51品茶（ 4.0.0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 | 51品茶 |
| 版本 | 4.0.0 |
| 包名 | com.example.chaguaner2023 |
| 域名线索 | 25条 |
| URL线索 | 15条 |
| APP图标 |  |
| 分析日期 | 2025年1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 | cg\_0719.apk |
| 文件大小 | 33.68MB |
| MD5值 | c1163fcc4e53869837aaf4124568a92b |
| SHA1值 | 5950ea5ed527503ff05f8ea7faf89eb9b577365a |
| SHA256值 | e81776265b1b4a3ccc993ffe44a85007caa7ddccc031aa579f432255946f3751 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 51品茶 |
| 包名 | com.example.chaguaner2023 |
| 主活动Activity | com.example.chaguaner2023.MainActivity |
| 安卓版本名称 | 4.0.0 |
| 安卓版本 | 400 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| aomedia.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| vbwtbv.wehzmsx.com | IP: 104.21.47.210 所属国家: United States of America 地区: California 城市: San Francisco  |
| scripts.sil.org | IP: 104.22.11.254 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| h0fr77y9.slt.sched.intlscdn.com | IP: 170.187.231.7 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| flutter.dev | IP: 199.36.158.100 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  |
| gitee.com | IP: 180.76.198.77 所属国家: China 地区: Beijing 城市: Beijing  |
| default.url | 没有服务器地理信息.  |
| exoplayer.dev | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| vbwtbv.uyijwwn.com | IP: 172.67.203.38 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| wvseee.jsbacjr.com | IP: 172.67.175.194 所属国家: United States of America 地区: California 城市: San Francisco  |
| raw.githubusercontent.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| api.flutter.dev | IP: 199.36.158.100 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: Singapore 地区: Singapore 城市: Singapore  |
| new1.wanzhuoli.top | IP: 122.189.171.115 所属国家: China 地区: Hubei 城市: Xiangyang  |
| www.ibm.com | IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| developer.android.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| android.googlesource.com | IP: 142.251.170.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| ns.adobe.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/c.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | e0/x0.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | b2/b0.java  |
| https://x</LA\_URL>  | j0/k0.java  |
| https://default.url  | j0/k0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | j0/l0.java  |
| http://dashif.org/guidelines/last-segment-number  | l1/d.java  |
| http://dashif.org/guidelines/trickmode  | l1/d.java  |
| http://dashif.org/thumbnail\_tile  | l1/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | l1/d.java  |
| http://ns.adobe.com/xap/1.0/  | p0/a.java  |
| https://aomedia.org/emsg/ID3  | z0/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | z0/a.java  |
| 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  |
| play.googleapis.com  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| http://www.unicode.org/copyright.html  | 摸瓜V3引擎  |
| vbwtbv.wehzmsx.com  | 摸瓜V3引擎  |
| http://scripts.sil.org/OFLhttp://scripts.sil.org/OFL  | 摸瓜V3引擎  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V3引擎  |
| h0fr77y9.slt.sched.intlscdn.com  | 摸瓜V3引擎  |
| https://aomedia.org/emsg/ID3  | 摸瓜V3引擎  |
| http://dashif.org/thumbnail\_tile  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/permissions/overview  | 摸瓜V3引擎  |
| https://github.com/flutter/flutter/issues.  | 摸瓜V3引擎  |
| wvseee.jsbacjr.com  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/trickmode  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/thumbnail\_tile  | 摸瓜V3引擎  |
| https://github.com/dart-lang/sdk/blob/master/runtime/docs/compiler/aot/entry\_point\_pragma.md  | 摸瓜V3引擎  |
| new1.wanzhuoli.top  | 摸瓜V3引擎  |
| https://github.com/apvarun/toastify-js  | 摸瓜V3引擎  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/last-segment-number  | 摸瓜V3引擎  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | 摸瓜V3引擎  |
| https://default.url  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| https://vbwtbv.wehzmsx.com  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://gitee.com/fdsaw/ffewelmcxww/raw/master/cg.txt  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| https://wvseee.jsbacjr.com/cg.txt  | lib/armeabi-v7a/libapp.so  |
| https://raw.githubusercontent.com/little-5/backup/master/cg.txt?t=  | lib/armeabi-v7a/libapp.so  |
| https://vbwtbv.uyijwwn.com  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues.  | 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  |
| \_growablelist@0150898.\_literal \_typeerror@0150898.\_create \_bytebuffer@7027147.\_new \_immutablelist@0150898.\_uk \_double@0150898.fromintege \_casterror@0150898.\_create \_assertionerror@0150898.\_create  | lib/armeabi-v7a/libapp.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | i2/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: CN=Android Debug, O=Android, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2024-02-10 07:12:47+00:00 有效期至: 2054-02-02 07:12:47+00:00 发行人: CN=Android Debug, O=Android, C=US 序列号: 0x1 哈希算法: sha256 md5值: 73e8a618da84833ebd3aed6d63a9ccaf sha1值: 8cfcf0fea89841747a1bd225f70d99045787e230 sha256值: 3700cee9dcef3c9e696aa51d4ad581b332fbc4040477853f7812ea91c75b75f0 sha512值: b59b74d1370c5509886a41046509857127a0839378b83926a43aa423d1bb45dea901907a9b8f1172ac0430536fa282687ee4c5f256e1e2e49b3dca070457338f 公钥算法: rsa 密钥长度: 2048 指纹: 5a3db976ca130f12887af21ec865966dadfba3e4e6c924570369047e0ede67fe**

## **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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| 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.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\_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.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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.example.chaguaner2023.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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。**