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

**TO-Remarkable1（ 1.3.0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 | TO-Remarkable1 |
| 版本 | 1.3.0 |
| 包名 | com.app.remark.repoact |
| 域名线索 | 46条 |
| URL线索 | 31条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 853-1752108496.apk |
| 文件大小 | 69.63MB |
| MD5值 | 6406e1a60ace9f18596090e5d7e3b313 |
| SHA1值 | 1bfc404be2038b87734a9c08413742f465b8a469 |
| SHA256值 | c489fd998bf838e3da0f463c321b1455810a71b7877f23daa6693333f4671538 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TO-Remarkable1 |
| 包名 | com.app.remark.repoact |
| 主活动Activity | com.app.remark.repoact.MainActivity |
| 安卓版本名称 | 1.3.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| check-ipv4.netease.im | IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| register.xmpush.global.xiaomi.com | IP: 47.237.96.1 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.  |
| wannos.127.net | IP: 45.127.129.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| www.example.com | IP: 23.193.186.17 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| nrtc.netease.im | IP: 220.197.34.71 所属国家: China 地区: Sichuan 城市: Leshan  |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| abt-online.netease.im | IP: 220.197.34.89 所属国家: China 地区: Sichuan 城市: Leshan  |
| resolver.msg.xiaomi.net | IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| resolver.msg.global.xiaomi.net | IP: 34.36.192.126 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| norma-external-collect.meizu.com | 没有服务器地理信息.  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| idmb.register.xmpush.global.xiaomi.com | IP: 20.219.205.9 所属国家: India 地区: Maharashtra 城市: Pune  |
| check-ipv6.netease.im | 没有服务器地理信息.  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| xmlpull.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| lbs.netease.im | IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| change-api.netease.im | IP: 220.197.34.84 所属国家: China 地区: Sichuan 城市: Leshan  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| statistic-overseas.yunxinfw.com | IP: 8.219.207.113 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| statistic.live.126.net | IP: 220.197.34.75 所属国家: China 地区: Sichuan 城市: Leshan  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| webtest.netease.im | IP: 111.124.202.79 所属国家: China 地区: Guizhou 城市: Zunyi  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| nosup-hz1.127.net | IP: 124.163.197.206 所属国家: China 地区: Shanxi 城市: Taiyuan  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| http://webtest.netease.im/nrtcproxy/nrtc/getSdkConfig.action  | com/netease/lava/nertc/foreground/Authenticate.java  |
| https://nrtc.netease.im/nrtc/getSdkConfig.action  | com/netease/lava/nertc/foreground/Authenticate.java  |
| https://statistic.live.126.net  | com/netease/nimlib/c.java  |
| https://statistic-overseas.yunxinfw.com  | com/netease/nimlib/c.java  |
| https://statistic.live.126.net  | com/netease/nimlib/net/a/d/a.java  |
| https://statistic-overseas.yunxinfw.com  | com/netease/nimlib/net/a/d/a.java  |
| https://abt-online.netease.im/v1/api/abt/client/getExperimentInfo  | com/netease/nimlib/abtest/c.java  |
| https://lbs.netease.im/lbs/conf.jsp  | com/netease/nimlib/d/e.java  |
| https://check-ipv4.netease.im/  | com/netease/nimlib/d/e.java  |
| https://check-ipv6.netease.im/  | com/netease/nimlib/d/e.java  |
| https://wannos.127.net/lbs  | com/netease/nimlib/d/g.java  |
| https://nosup-hz1.127.net  | com/netease/nimlib/d/g.java  |
| https://change-api.netease.im/change-api/sdk/task/action/batch  | com/netease/yunxin/artemis/ArtemisTask/YXArtemisPullTask.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fv.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gg.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gn.java  |
| https://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/go.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fj.java  |
| https://resolver.msg.global.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | e1/z.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | k/b1.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | j5/m.java  |
| http://dashif.org/guidelines/last-segment-number  | o0/d.java  |
| http://dashif.org/guidelines/trickmode  | o0/d.java  |
| http://dashif.org/thumbnail\_tile  | o0/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | o0/d.java  |
| https://github.com/Baseflow/flutter-permission-handler/issues  | g/n.java  |
| https://github.com/bluefireteam/audioplayers/blob/main/troubleshooting.md  | k5/o.java  |
| http://ns.adobe.com/xap/1.0/  | u/a.java  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 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**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | k1/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=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-26 08:47:56+00:00 有效期至: 2046-10-20 08:47:56+00:00 发行人: C=000000, ST=openim, L=openim, O=openim, OU=openim, CN=openim 序列号: 0x19e05291 哈希算法: sha256 md5值: 05d03bd8459d4a87134eb128e3dab5fd sha1值: 57ce8b8feb004052692f721f7ffa52be51def128 sha256值: 1f38a82fb3c33be7951fb5d964ef5bd9c6c9bfc084ae1e2a8a40a0d1f44ae1fe sha512值: 797e3ccaf31be41cfce915486e9027118413d22103ba02737cf0ae37904874a7791ab675fb4508cf7b9edfa6044393cb1e282f99eb133f515fe1afdc2447cc0d 公钥算法: rsa 密钥长度: 2048 指纹: 0b749ba3321060732b29f063fbabeb507e14e7e949653bdabdbd3bd3139c14e2**

## **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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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 |
| 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.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.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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| com.app.remark.repoact.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.permission.READ\_SDID\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.app.remark.repoact.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.app.remark.repoact.permission.PUSH\_PROVIDER | 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。**