



MoGua

TO-Remarkable1 1.3.0.APK 分析报告



APP名称:

TO-Remarkable1

包名:	com.app.remark.repoact
域名线索:	46条
URL线索:	31条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件名: 853-1752108496.apk

文件大小: 69.63MB

MD5值: 6406e1a60ace9f18596090e5d7e3b313

SHA1值: 1bfc404be2038b87734a9c08413742f465b8a469

SHA256值: c489fd998bf838e3da0f463c321b1455810a71b7877f23daa6693333f4671538

i APP 信息

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

🔍 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 纬度: 39.907501 经度: 116.397102
api-push.meizu.com	IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan 纬度: 23.026770 经度: 113.131477
	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania

dashif.org	城市: California 纬度: 40.065647 经度: -79.891724
check-ipv4.netease.im	IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
register.xmpush.global.xiaomi.com	IP: 47.237.96.1 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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 纬度: 23.127361 经度: 113.264572
www.jivesoftware.com	IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach 纬度: 36.837925

	经度: -76.093918
www.example.com	IP: 23.193.186.17 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
nrtc.netease.im	IP: 220.197.34.71 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
fr.register.xmpush.global.xiaomi.com	IP: 98.64.182.160 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.378502 经度: 4.899980
abt-online.netease.im	IP: 220.197.34.89 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
resolver.msg.xiaomi.net	IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 49.4.40.185 所属国家: China

grs.dbankcloud.asia	地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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 纬度: 39.099731 经度: -94.578568
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 纬度: 1.289987 经度: 103.850281
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 纬度: 18.519663 经度: 73.854507
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 纬度: 55.752258

	经度: 37.615471
xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.jsdelivr.com	IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
metrics5.dt.dbankcloud.ru	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
lbs.netease.im	IP: 220.197.34.90 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
api-push.in.meizu.com	IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon 纬度: 38.978210 经度: -77.386993
	IP: 159.138.202.31 所属国家: Russian Federation

data-drru.push.dbankcloud.com	地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
data-dre.push.dbankcloud.com	IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
change-api.netease.im	IP: 220.197.34.84 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
cn.register.xmpush.xiaomi.com	IP: 123.125.102.39 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

play.google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
statistic-overseas.yunxinfw.com	IP: 8.219.207.113 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
developer.android.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
metrics2.data.hicloud.com	IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel

	纬度: 54.321358 经度: 10.134532
appgallery.cloud.huawei.com	IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
statistic.live.126.net	IP: 220.197.34.75 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
data-drcn.push.dbankcloud.com	IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
webtest.netease.im	IP: 111.124.202.79 所属国家: China 地区: Guizhou 城市: Zunyi 纬度: 27.686441 经度: 106.907135
metrics5.data.hicloud.com	IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
	IP: 124.163.197.206

nosup-hz1.127.net

所属国家: China
地区: Shanxi
城市: Taiyuan
纬度: 37.869438
经度: 112.561508

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/nrtc/foreground/Authenticate.java
https://nrtc.netease.im/nrtc/getSdkConfig.action	com/netease/lava/nrtc/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

✉ 邮箱线索

☰ 手机线索

手机号	所在文件
17512775099	k1/a.java

✿ 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

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。