MoGua

IVOJI 3.0.22.APK 分析报告

APP名称:	IVOJI

包名:	id.ivoji
域名线索:	50条
URL线索:	26条
邮箱线索:	0条
分析日期:	2025年7月31日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: ivojiapp-v30022-20250709-GooglePlay-release.apk
文件大小: 16.16MB
MD5值: 5d6a62ffd2c336cb84f0686d2fc297fd
SHA1值: 573170820594bfe8d84f86bab74eb7cafa87ebea
SHA256值: 5db2ac84af8dadb8c02ab845331c69fe8adaef2e953e0fc7504c78bd288cd8ff

APP 信息

App名称: IVOJI
包名: id.ivoji
主活动Activity: com.ivoji.commonlibrary.ui.WelcomeActivity
安卓版本名称: 3.0.22
安卓版本: 30022

域名线索

域名	服务器信息
youtrack.jetbrains.com	**IP**: 63.35.30.167 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
ssdk-services.s	没有服务器地理信息.
scdn-ssettings.s	没有服务器地理信息.
appv.ivoji.id	**IP**: 149.129.235.56 **所属国家**: Indonesia **地区**: Jakarta Raya **城市**: Jakarta **纬度**: -6.208678 **经度**: 106.845490

scdn-stestsettings.s	没有服务器地理信息.
slaunches.s	没有服务器地理信息.
app.adjust.world	**IP**: 185.151.204.40 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
sonelink.s	没有服务器地理信息.
gdpr.adjust.net.in	**IP**: 185.151.204.30 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
.facebook.com	没有服务器地理信息.
sconversions.s	没有服务器地理信息.
aps-webhandler.appsflyer.com	**IP**: 13.226.210.103 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
simpression.s	没有服务器地理信息.
sapp.s	没有服务器地理信息.
sars.s	没有服务器地理信息.

sadrevenue.s	没有服务器地理信息.
graph.s	没有服务器地理信息.
subscription.us.adjust.com	**IP**: 185.151.204.70 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
gdpr.us.adjust.com	**IP**: 185.151.204.70 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
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
gdpr.tr.adjust.com	**IP**: 195.244.54.5 **所属国家**: Turkey **地区**: Izmir **城市**: Izmir **纬度**: 38.412731 **经度**: 27.138380
schemas.android.com	没有服务器地理信息.
graph-video.s	没有服务器地理信息.
	IP: 185.151.204.7

app.adjust.com	**所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
subscription.adjust.world	**IP**: 185.151.204.44 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
subscription.tr.adjust.com	**IP**: 195.244.54.5 **所属国家**: Turkey **地区**: Izmir **城市**: Izmir **纬度**: 38.412731 **经度**: 27.138380
sinapps.s	没有服务器地理信息.
app.adjust.net.in	**IP**: 185.151.204.32 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
gdpr.eu.adjust.com	**IP**: 185.151.204.60 **所属国家**: Germany **地区**: Berlin

	城市: Berlin **纬度**: 52.524525 **经度**: 13.410037
developers.facebook.com	**IP**: 162.125.34.133 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
subscription.eu.adjust.com	**IP**: 185.151.204.60 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
gdpr.adjust.world	**IP**: 185.151.204.40 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
subscription.adjust.com	**IP**: 185.151.204.52 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
smonitorsdk.s	没有服务器地理信息.
app.tr.adjust.com	**IP**: 195.244.54.5 **所属国家**: Turkey **地区**: Izmir **城市**: Izmir **纬度**: 38.412731

	经度: 27.138380
sregister.s	没有服务器地理信息.
gdpr.adjust.com	**IP**: 185.151.204.50 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
sgcdsdk.s	没有服务器地理信息.
svalidate.s	没有服务器地理信息.
app.us.adjust.com	**IP**: 185.151.204.70 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
sattr.s	没有服务器地理信息.
subscription.adjust.net.in	**IP**: 185.151.204.34 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
overmind.datatheorem.com	**IP**: 142.250.69.179 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514

sdlsdk.s	没有服务器地理信息.
app.adjust.cn	**IP**: 47.104.30.117 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
app.eu.adjust.com	**IP**: 185.151.204.60 **所属国家**: Germany **地区**: Berlin **城市**: Berlin **纬度**: 52.524525 **经度**: 13.410037
svalidate-and-log.s	没有服务器地理信息.
facebook.com	**IP**: 173.236.212.42 **所属国家**: United States of America **地区**: California **城市**: Brea **纬度**: 33.930222 **经度**: -117.888420
sviap.s	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://app.adjust.com	com/adjust/sdk/Constants.java
https://gdpr.adjust.com	com/adjust/sdk/Constants.java

https://subscription.adjust.com	com/adjust/sdk/Constants.java
https://github.com/adjust/android_sdk	com/adjust/sdk/ActivityHandler.java
https://app.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://app.adjust.cn	com/adjust/sdk/network/UrlStrategy.java
https://app.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://app.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java

https://subscription.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://aps-webhandler.appsflyer.com/api/trigger	com/appsflyer/internal/AFj1mSDK.java
https://appv.ivoji.id/index.html	com/ivoji/commonlibrary/ui/WelcomeActivity.java
http://schemas.android.com/apk/res/android	defpackage/xe.java
http://schemas.android.com/apk/res/android	defpackage/ip0.java
https://developers.facebook.com/docs/android/getting-started	defpackage/yv.java
https://graph-video.%s	defpackage/yv.java
https://graph.%s	defpackage/yv.java
https://youtrack.jetbrains.com/issue/KT-55980	defpackage/ub0.java
https://overmind.datatheorem.com/trustkit/report	defpackage/wl.java
https://developers.facebook.com/docs/android/troubleshooting/	defpackage/k70.java
https://developers.facebook.com/docs/app-events/getting-started-app-events-android	defpackage/ro0.java
https://facebook.com/device?user_code=%1$s&qr=1	defpackage/xk.java
http://schemas.android.com/apk/res/android	defpackage/vn0.java
https://graph.%s	defpackage/ln.java
http://schemas.android.com/apk/res/android	defpackage/c9.java

https://developers.facebook.com/docs/android/getting-started	defpackage/cl.java
https://facebook.com	defpackage/ow.java
https://.facebook.com	defpackage/ow.java
http://xml.apache.org/xslt	defpackage/ow.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	defpackage/d50.java

邮箱线索

手机线索

手机号	所在文件
15552000000	defpackage/d50.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=ID, ST=DKI Jakarta, L=Jakarta, O=Finansia Aira Teknologi, OU=IVOJI, CN=Finansia Aira Teknologi
签名算法: rsassa_pkcs1v15
有效期自: 2020-02-29 16:43:41+00:00
有效期至: 2047-07-17 16:43:41+00:00
发行人: C=ID, ST=DKI Jakarta, L=Jakarta, O=Finansia Aira Teknologi, OU=IVOJI, CN=Finansia Aira Teknologi
序列号: 0x6ca859ed

哈希算法: sha256
md5值: 6fe4428f0ff07c2b9593118085bc378a
sha1值: aa810bbc9b3a6af638366a97d0e1b840f2579a34
sha256值: 0f020edc8458f1680942d967e6e5a8685d5eaea9f5dec76a5c72429459e3201e
sha512值: eff386b1d8e928c6b599288c61256241da057659cc174411b443f224ebefe388d03dfac6dab8810bb03d09861cb5e33b7914a6cb645f4076a62abcff9b819ed8
公钥算法: rsa
密钥长度: 2048
指纹: f2a404097d324743ad2710d4cf8cd87c8389b56b2863cc25fcb4f34a65d5534c

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

	是否		

向手机申请的权限	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_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.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.POST_NOTIFICATIONS	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.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.HIGH_SAMPLING_RATE_SENSORS	正常	访问更高采样率的传感器数据	允许应用访问采样率大于 200 Hz 的传感器数据
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference
id.ivoji.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	未知	Unknown permission	Unknown permission from android reference

com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.facebook.CustomTabActivity	Schemes: @string/FACEBOOK_LOGIN_SCHEMA://, fbconnect://, Hosts: cct.id.ivoji,

---

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。