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

**TBot（ 1.7.8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 | TBot |
| 版本 | 1.7.8 |
| 包名 | it.ppndrd.taskbot |
| 域名线索 | 68条 |
| URL线索 | 71条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | TBot - a powerful AI assistant\_1.7.8\_APKPure.apk |
| 文件大小 | 77.66MB |
| MD5值 | 9c686010928db4a33121c179b794d032 |
| SHA1值 | a377708759e8f561f7a52cf72791865747554591 |
| SHA256值 | 125f3b66ea25d99cfe597e5a4517bee6c606c6691c851b9390e9fef385a51aba |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | TBot |
| 包名 | it.ppndrd.taskbot |
| 主活动Activity | it.ppndrd.taskbot.MainActivity |
| 安卓版本名称 | 1.7.8 |
| 安卓版本 | 72 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| rt.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| ms.applovin.com | IP: 34.102.162.219 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| schemas.android.com | 没有服务器地理信息.  |
| android.googlesource.com | IP: 74.125.23.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.huawei.com | IP: 123.125.16.228 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.com | IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| a.applovin.com | IP: 34.117.147.68 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| play.google | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| appgallery.huawei.com | IP: 49.4.34.28 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| symbolize.corp.google.com | IP: 108.177.125.129 所属国家: United States of America 地区: California 城市: Mountain View  |
| bit.ly | IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| twitter.com | IP: 199.96.58.85 所属国家: United States of America 地区: California 城市: San Francisco  |
| rt.applvn.com | IP: 104.17.2.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| firebaseremoteconfig.googleapis.com | IP: 142.251.42.234 所属国家: United States of America 地区: California 城市: Mountain View  |
| vid.applovin.com | IP: 34.160.64.118 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| market.android | 没有服务器地理信息.  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| d.applvn.com | IP: 104.17.2.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| mobile.maps | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.applovin.com | 没有服务器地理信息.  |
| www.mopub.com | IP: 34.111.170.5 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| firebaseinstallations.googleapis.com | IP: 142.251.42.234 所属国家: United States of America 地区: California 城市: Mountain View  |
| d.applovin.com | IP: 34.110.179.88 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| m.maps | 没有服务器地理信息.  |
| developers.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| aomedia.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.ibm.com | IP: 2.18.159.141 所属国家: France 地区: Ile-de-France 城市: Paris  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| assets.applovin.com | IP: 34.120.175.182 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| play.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| adlib-mock.yandex.net | IP: 213.180.193.100 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| store.hispace.hicloud.com | IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| maps.yandex.ru | IP: 213.180.204.242 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| ms.applvn.com | IP: 104.17.2.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.apple.com | IP: 17.253.87.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.peoplendroid.it | IP: 217.64.195.181 所属国家: Italy 地区: Lazio 城市: Frosinone  |
| prod-a.applovin.comhttps | 没有服务器地理信息.  |
| store-drru.hispace.hicloud.com | IP: 159.138.202.186 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| store3.hispace.hicloud.com | IP: 23.3.104.100 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| startup.mobile.yandex.net | IP: 213.180.204.244 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| www.facebook.com | IP: 104.244.46.63 所属国家: United States of America 地区: California 城市: San Francisco  |
| a.applvn.com | IP: 104.17.2.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| openai.com | IP: 104.18.33.45 所属国家: United States of America 地区: California 城市: San Francisco  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mobile.yandexadexchange.net | IP: 213.180.193.198 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| monetization-support.applovin.com | IP: 34.110.151.135 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| tech.yandex.com | IP: 213.180.204.242 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| yandex.ru | IP: 5.255.255.77 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| store1.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.amazon.com | IP: 13.32.53.28 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| developer.android.com | IP: 142.251.42.238 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.  |
| fonts.gstatic.com | IP: 203.208.49.98 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| firebase.google.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| store2.hispace.hicloud.com | IP: 18.65.168.75 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://applovin.com.  | defpackage/am.java  |
| http://schemas.android.com/apk/res/android  | defpackage/cs3.java  |
| https://play.google.com/store/apps/details?id=  | defpackage/cy4.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | defpackage/d80.java  |
| http://dashif.org/guidelines/last-segment-number  | defpackage/d40.java  |
| http://dashif.org/guidelines/trickmode  | defpackage/d40.java  |
| https://firebaseinstallations.googleapis.com/v1  | defpackage/ei1.java  |
| https://developer.android.com/reference/com/google/android/play/core/splitinstall/model/SplitInstallErrorCode.html  | defpackage/gw3.java  |
| https://developer.android.com/reference/com/google/android/play/core/assetpacks/model/AssetPackErrorCode.html  | defpackage/hr3.java  |
| https://github.com/google/guava/issues/5269  | defpackage/jy3.java  |
| https://bit.ly/2XFpdma  | defpackage/kd4.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | defpackage/j5.java  |
| http://www.w3.org/ns/ttml  | defpackage/l60.java  |
| https://firebaseremoteconfig.googleapis.com/v1/projects/%s/namespaces/%s:fetch  | defpackage/pj1.java  |
| https://bit.ly/2XFpdma  | defpackage/rd4.java  |
| https://developer.android.com/training/articles/security-config  | defpackage/sl.java  |
| http://schemas.android.com/apk/res/android  | defpackage/x1.java  |
| http://ns.adobe.com/xap/1.0/  | defpackage/xy.java  |
| https://ms.applovin.com/  | defpackage/ym.java  |
| https://ms.applvn.com/  | defpackage/ym.java  |
| https://monetization-support.applovin.com/hc/en-us/articles/236114328-How-can-I-expose-verbose-logging-for-the-SDK>  | defpackage/yn.java  |
| https://vid.applovin.com/,https://pdn.applovin.com/,https://img.applovin.com/,https://d.applovin.com/,https://assets.applovin.com/,https://cdnjs.cloudflare.com/,http://vid.applovin.com/,http://pdn.applovin.com/,http://img.applovin.com/,http://d.applovin.com/,http://assets.applovin.com/,http://cdnjs.cloudflare.com/  | defpackage/zm.java  |
| https://prod-a.applovin.com,https://rt.applovin.com/4.0/pix,  | defpackage/zm.java  |
| https://rt.applvn.com/4.0/pix,https://ms.applovin.com/,https://ms.applvn.com/  | defpackage/zm.java  |
| https://ms.applovin.com/  | defpackage/zm.java  |
| https://ms.applvn.com/  | defpackage/zm.java  |
| https://a.applovin.com/  | defpackage/zm.java  |
| https://a.applvn.com/  | defpackage/zm.java  |
| https://d.applovin.com/  | defpackage/zm.java  |
| https://d.applvn.com/  | defpackage/zm.java  |
| https://rt.applovin.com/  | defpackage/zm.java  |
| https://rt.applvn.com/  | defpackage/zm.java  |
| https://assets.applovin.com/gdpr/flow\_v1/gdpr-flow-1.html  | defpackage/zm.java  |
| http://schemas.applovin.com/android/1.0  | com/applovin/adview/AppLovinAdView.java  |
| https://blank  | com/applovin/impl/sdk/y.java  |
| http://developer.android.com/google/play-services/setup.html.  | com/applovin/impl/sdk/m.java  |
| http://schemas.android.com/apk/res/android  | com/applovin/mediation/ads/MaxAdView.java  |
| https://www.huawei.com/auth/account/nonincludegranted  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile/accesstoken  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/carrierid  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile/serviceauthcode  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/base.profile  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/country  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/games  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/shipping.address  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/age.range  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/assisttoken  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/homezone  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/age.groupflag  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/mobile.flag  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/mobile.number  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/account/realname.anonymous  | com/huawei/hms/support/api/entity/common/CommonConstant.java  |
| https://www.huawei.com/auth/pay/walletinfo  | com/huawei/hms/support/api/pay/HuaweiPay.java  |
| https://play.google.com/store/apps/details?%s  | com/mopub/common/util/Intents.java  |
| https://www.amazon.com/gp/mas/dl/android?%s  | com/mopub/common/util/Intents.java  |
| https://twitter.com/%s/status/%s  | com/mopub/common/util/Intents.java  |
| https://www.mopub.com/optout  | com/mopub/nativeads/MoPubCustomEventNative.java  |
| https://startup.mobile.yandex.net/  | com/yandex/metrica/impl/ob/Uu.java  |
| https://tech.yandex.com/metrica-mobile-sdk/doc/mobile-sdk-dg/concepts/android-initialize-docpage/  | com/yandex/metrica/impl/ob/C1607fD.java  |
| https://yandex.ru/appcry  | com/yandex/mobile/ads/impl/avw.java  |
| https://mobile.yandexadexchange.net  | com/yandex/mobile/ads/impl/axt.java  |
| http://xmlpull.org/v1/doc/features.html  | com/yandex/mobile/ads/impl/ayv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/yandex/mobile/ads/impl/azk.java  |
| https://market.android  | com/yandex/mobile/ads/impl/gj.java  |
| http://market.android  | com/yandex/mobile/ads/impl/gj.java  |
| https://play.google  | com/yandex/mobile/ads/impl/gj.java  |
| http://play.google  | com/yandex/mobile/ads/impl/gj.java  |
| https://map  | com/yandex/mobile/ads/impl/gj.java  |
| http://map  | com/yandex/mobile/ads/impl/gj.java  |
| https://maps  | com/yandex/mobile/ads/impl/gj.java  |
| http://maps  | com/yandex/mobile/ads/impl/gj.java  |
| http://mobile.maps  | com/yandex/mobile/ads/impl/gj.java  |
| http://m.maps  | com/yandex/mobile/ads/impl/gj.java  |
| http://maps.yandex.ru  | com/yandex/mobile/ads/impl/gj.java  |
| https://mobile.yandexadexchange.net  | com/yandex/mobile/ads/impl/ji.java  |
| https://adlib-mock.yandex.net  | com/yandex/mobile/ads/impl/kc.java  |
| https://yandex.ru/dev/mobile-ads/doc/android/quick-start/android-ads-component.html  | com/yandex/mobile/ads/impl/lx.java  |
| https://yandex.ru/dev/mobile-ads/doc/intro/changelog-android.html  | com/yandex/mobile/ads/impl/lx.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | com/yandex/mobile/ads/impl/nc.java  |
| https://aomedia.org/emsg/ID3  | com/yandex/mobile/ads/impl/tl.java  |
| https://developer.apple.com/streaming/emsg-id3  | com/yandex/mobile/ads/impl/tl.java  |
| https://yandex.ru  | com/yandex/mobile/ads/impl/y.java  |
| http://www.w3.org/ns/ttml  | com/yandex/mobile/ads/impl/wi.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://github.com/flutter/flutter/issues/2897).It  | io/flutter/plugin/platform/PlatformViewsController.java  |
| https://github.com/flutter/plugins/blob/master/packages/in\_app\_purchase/in\_app\_purchase/README.md  | io/flutter/plugins/inapppurchase/MethodCallHandlerImpl.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects  | io/flutter/view/FlutterView.java  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |
| https://firebase.google.com/support/privacy  | lib/arm64-v8a/libapp.so  |
| https://developers.google.com/terms/  | lib/arm64-v8a/libapp.so  |
| https://www.facebook.com/ppndrdapps/  | lib/arm64-v8a/libapp.so  |
| https://www.peoplendroid.it/tbot  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/libapp.so  |
| https://appgallery.huawei.com/  | lib/arm64-v8a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/arm64-v8a/libapp.so  |
| https://www.peoplendroid.it/REST/tbot/index.php  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/2000/svg  | lib/arm64-v8a/libapp.so  |
| https://www.peoplendroid.it/privacy/TBot-PrivacyPolicy.html  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/1999/xhtml  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/1998/Math/MathML  | lib/arm64-v8a/libapp.so  |
| https://openai.com  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/libapp.so  |
| https://www.peoplendroid.it/REST/tbot/translator.php  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/1999/xlink  | lib/arm64-v8a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/arm64-v8a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/arm64-v8a/libapp.so  |
| https://fonts.gstatic.com/s/a/  | lib/arm64-v8a/libapp.so  |
| 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.  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues/73620.  | lib/arm64-v8a/libflutter.so  |
| https://github.com/opencv/opencv/issues/6293  | lib/arm64-v8a/libmlkit-label-MS.so  |
| http://b/24559754.  | lib/arm64-v8a/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/arm64-v8a/libmlkitcommonpipeline.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/arm64-v8a/libmlkitcommonpipeline.so  |
| https://developer.android.com/reference/android/content/Context.html  | lib/arm64-v8a/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/arm64-v8a/libtranslate\_jni.so  |
| https://firebase.google.com/support/privacy  | lib/armeabi-v7a/libapp.so  |
| https://developers.google.com/terms/  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| https://appgallery.huawei.com/  | lib/armeabi-v7a/libapp.so  |
| https://www.peoplendroid.it/tbot  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| https://www.peoplendroid.it/REST/tbot/index.php  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/svg  | lib/armeabi-v7a/libapp.so  |
| https://www.peoplendroid.it/privacy/TBot-PrivacyPolicy.html  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/1998/Math/MathML  | lib/armeabi-v7a/libapp.so  |
| https://openai.com  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://www.peoplendroid.it/privacy/TBot-TermsAndConditions.html  | 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/new.  | lib/armeabi-v7a/libapp.so  |
| https://fonts.gstatic.com/s/a/  | lib/armeabi-v7a/libapp.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.  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues/73620.  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/opencv/opencv/issues/6293  | lib/armeabi-v7a/libmlkit-label-MS.so  |
| http://b/24559754.  | lib/armeabi-v7a/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/armeabi-v7a/libmlkitcommonpipeline.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libmlkitcommonpipeline.so  |
| https://developer.android.com/reference/android/content/Context.html  | lib/armeabi-v7a/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/armeabi-v7a/libtranslate\_jni.so  |
| http://b/24559754.  | lib/x86/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/x86/libmlkitcommonpipeline.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86/libmlkitcommonpipeline.so  |
| https://developer.android.com/reference/android/content/Context.html  | lib/x86/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/x86/libtranslate\_jni.so  |
| https://firebase.google.com/support/privacy  | lib/x86\_64/libapp.so  |
| https://developers.google.com/terms/  | lib/x86\_64/libapp.so  |
| https://www.facebook.com/ppndrdapps/  | lib/x86\_64/libapp.so  |
| https://www.peoplendroid.it/tbot  | lib/x86\_64/libapp.so  |
| http://www.w3.org/XML/1998/namespace  | lib/x86\_64/libapp.so  |
| https://appgallery.huawei.com/  | lib/x86\_64/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/x86\_64/libapp.so  |
| https://www.peoplendroid.it/REST/tbot/index.php  | lib/x86\_64/libapp.so  |
| http://www.w3.org/2000/svg  | lib/x86\_64/libapp.so  |
| https://www.peoplendroid.it/privacy/TBot-PrivacyPolicy.html  | lib/x86\_64/libapp.so  |
| http://www.w3.org/1999/xhtml  | lib/x86\_64/libapp.so  |
| http://www.w3.org/1998/Math/MathML  | lib/x86\_64/libapp.so  |
| https://openai.com  | lib/x86\_64/libapp.so  |
| http://www.w3.org/2000/xmlns/  | lib/x86\_64/libapp.so  |
| https://www.peoplendroid.it/REST/tbot/translator.php  | lib/x86\_64/libapp.so  |
| http://www.w3.org/1999/xlink  | lib/x86\_64/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/x86\_64/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/x86\_64/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/x86\_64/libapp.so  |
| https://fonts.gstatic.com/s/a/  | lib/x86\_64/libapp.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/x86\_64/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | 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://b/24559754.  | lib/x86\_64/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/x86\_64/libmlkitcommonpipeline.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86\_64/libmlkitcommonpipeline.so  |
| https://developer.android.com/reference/android/content/Context.html  | lib/x86\_64/libmlkitcommonpipeline.so  |
| https://symbolize.corp.google.com/r/?trace=  | lib/x86\_64/libtranslate\_jni.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| support@mopub.com  | com/mopub/common/privacy/PersonalInfoManager.java  |
| \_httpparser@13463476.responsepa storationinformation@763124995.fromserial lectiontoolbarbutton@487113492.text \_socket@14069316.\_writepipe lectiontoolbarbutton@369392285.text \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_bigintimpl@0150898.\_fromint \_list@0150898.filled \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_internetaddress@14069316.fromstring \_list@0150898.empty \_directory@14069316.fromrawpat \_casterror@0150898.\_create \_invocationmirror@0150898.\_withtype \_rawsocket@14069316.\_writepipe \_colorfilter@15065589.lineartosr \_uri@0150898.file \_growablelist@0150898.\_literal1 \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of \_colorfilter@15065589.matrix \_list@0150898.\_ofimmutab \_utf8encoder@9003594.withbuffer \_nativesocket@14069316.pipe \_growablelist@0150898.\_ofimmutab \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_growablelist@0150898.\_withdata \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_list@0150898.\_oflist \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe \_immutablemap@0150898.\_create \_socket@14069316.\_readpipe \_list@0150898.\_ofother ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_filestream@14069316.forstdin \_colorfilter@15065589.srgbtoline \_immutablelist@0150898.\_from \_uri@0150898.directory \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee \_growablelist@0150898.\_oflist  | lib/arm64-v8a/libapp.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| android-sdk-releaser@ljlg19.prod  | lib/arm64-v8a/libmlkitcommonpipeline.so  |
| appro@openssl.org  | lib/arm64-v8a/libtranslate\_jni.so  |
| l@\_dashoffsettype.percentage \_httpparser@13463476.responsepa storationinformation@763124995.fromserial lectiontoolbarbutton@487113492.text lectiontoolbarbutton@369392285.text \_double@0150898.fromintege .\_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat c\_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode z\_timer@1026248.periodic m\_growablelist@0150898.\_literal2 g\_bigintimpl@0150898.from \_list@0150898.empty l@boxwidthstyle.tight \_directory@14069316.fromrawpat \_casterror@0150898.\_create l\_invocationmirror@0150898.\_withtype i\_rawsocket@14069316.\_writepipe \_colorfilter@15065589.lineartosr 4\_uri@0150898.file \_growablelist@0150898.\_literal1 \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 bb\_growablelist@0150898.\_ofgrowabl x\_growablelist@0150898.of 3\_list@0150898.\_ofimmutab v\_utf8encoder@9003594.withbuffer \_nativesocket@14069316.pipe \_growablelist@0150898.\_ofimmutab \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_list@0150898.of \_growablelist@0150898.\_withdata \_list@0150898.generate n\_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_literal3 u\_growablelist@0150898.\_ofother \_list@0150898.\_oflist \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe \_immutablemap@0150898.\_create \_socket@14069316.\_readpipe \_list@0150898.\_ofother eo\_bytebuffer@7027147.\_new ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create av\_nativesocket@14069316.normal j\_filestream@14069316.forstdin x\_colorfilter@15065589.srgbtoline \_uri@0150898.directory qd\_growablelist@0150898.\_literal8 v\_file@14069316.fromrawpat gh\_growablelist@0150898.generate \_uri@0150898.notsimple 7u\_growablelist@0150898.\_literal7 \_\_growablelist@0150898.\_ofefficie \_future@4048458.immediatee m\_growablelist@0150898.\_oflist  | lib/armeabi-v7a/libapp.so  |
| android-sdk-releaser@ljlg19.prod  | lib/armeabi-v7a/libmlkitcommonpipeline.so  |
| android-sdk-releaser@ljlg19.prod  | lib/x86/libmlkitcommonpipeline.so  |
| \_httpparser@13463476.responsepa storationinformation@763124995.fromserial lectiontoolbarbutton@487113492.text \_socket@14069316.\_writepipe lectiontoolbarbutton@369392285.text \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_bigintimpl@0150898.\_fromint \_list@0150898.filled \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_internetaddress@14069316.fromstring \_list@0150898.empty \_directory@14069316.fromrawpat \_casterror@0150898.\_create \_invocationmirror@0150898.\_withtype \_rawsocket@14069316.\_writepipe \_colorfilter@15065589.lineartosr \_uri@0150898.file \_growablelist@0150898.\_literal1 \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of \_colorfilter@15065589.matrix \_list@0150898.\_ofimmutab \_utf8encoder@9003594.withbuffer \_nativesocket@14069316.pipe \_growablelist@0150898.\_ofimmutab \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_growablelist@0150898.\_withdata \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_list@0150898.\_oflist \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe \_immutablemap@0150898.\_create \_socket@14069316.\_readpipe \_list@0150898.\_ofother ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_filestream@14069316.forstdin \_colorfilter@15065589.srgbtoline \_immutablelist@0150898.\_from \_uri@0150898.directory \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee \_growablelist@0150898.\_oflist  | lib/x86\_64/libapp.so  |
| android-sdk-releaser@ljlg19.prod  | lib/x86\_64/libmlkitcommonpipeline.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | defpackage/w04.java  |
| 18584484968  | lib/armeabi-v7a/libapp.so  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2021-03-16 09:17:53+00:00 有效期至: 2051-03-16 09:17:53+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xb8ea946df83f3809215a5a55ccd1f3d939660fec 哈希算法: sha256 md5值: 69025ee82589eafcd3461dabf6614ea3 sha1值: 76d1b8738e5b0479f4f24b3071da7550412c4a06 sha256值: 16476575973544f9fd65ec8fd6eb1ea499af3ecca38abaeb685e877c625b73c7 sha512值: b653a4617e29e4ee54cfac916d1035a52d2a66b6545c8df78767ab8278b1b93a520f0fff45c0d99e4245c0da427470ee70e3a567d91081649fc6111ec93411b5 公钥算法: rsa 密钥长度: 4096 指纹: 9bd7c0c1d67d29c17befab3c1db05bbb7cbb5b6c49573ee0e527247921201058**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "google\_api\_key" : "AIzaSyCEoRcF6qkCrT0f1qKHlNOJblqLso51ti8"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyCEoRcF6qkCrT0f1qKHlNOJblqLso51ti8"  |

## **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.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 |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| 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。 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.facebook.CustomTabActivity | **Schemes**: @string/fb\_login\_protocol\_scheme://,  |
| com.huawei.openalliance.ad.activity.PPSLauncherActivity | **Schemes**: hwpps://, **Hosts:** it.ppndrd.taskbot,  |

**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。**