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

**None（ 6.73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 | None |
| 版本 | 6.73 |
| 包名 | com.uptodown |
| 域名线索 | 22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 | uptodown-com.voicechat.whisper.apk |
| 文件大小 | 11.87MB |
| MD5值 | e3172ea97543b53b516fa56c6dc5ede2 |
| SHA1值 | 7702a902db789f731f92f1e1ead141c02805945f |
| SHA256值 | e44cf605c245910c3d1851e2c2aaadec96a23d8295f93bbaef0163b29316e959 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | None |
| 包名 | com.uptodown |
| 主活动Activity | com.uptodown.activities.MainActivity |
| 安卓版本名称 | 6.73 |
| 安卓版本 | 673 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| m.uptodown.net | IP: 151.101.91.52 所属国家: United States of America 地区: California 城市: San Francisco  |
| firebase.google.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| cmp.inmobi.com | IP: 3.169.183.40 所属国家: United States of America 地区: Washington 城市: Seattle  |
| gist.github.com | IP: 8.7.198.45 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| firebase-settings.crashlytics.com | IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing  |
| secure.uptodown.com | IP: 156.233.67.243 所属国家: South Africa 地区: Gauteng 城市: Johannesburg  |
| accounts.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| t.uptodown.app | IP: 162.125.80.3 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.virustotal.com | IP: 34.54.88.138 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| u.uptodown.app | IP: 69.171.229.73 所属国家: United States of America 地区: California 城市: Menlo Park  |
| adservice.google.com | IP: 114.250.64.38 所属国家: China 地区: Beijing 城市: Beijing  |
| api.cmp.inmobi.com | IP: 54.93.147.55 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| www.youtube.com | IP: 31.13.94.10 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| uptodown-android.uptodown.com | IP: 128.242.240.244 所属国家: United States of America 地区: Washington 城市: Redmond  |
| pagead2.googlesyndication.com | IP: 114.250.64.38 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.microsoft.com | IP: 13.107.253.39 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| www.uptodown.app | IP: 31.13.112.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| dw.uptodown.com | IP: 108.160.172.208 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.uptodown.com | IP: 162.125.8.1 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://accounts.google.com/o/oauth2/revoke?token=  | G/f.java  |
| https://cmp.inmobi.com/  | X3/n.java  |
| https://cmp.inmobi.com/  | X3/d.java  |
| https://cmp.inmobi.com/  | X3/p.java  |
| https://cmp.inmobi.com/  | X3/l.java  |
| https://cmp.inmobi.com/  | X3/r.java  |
| https://cmp.inmobi.com/  | X3/t.java  |
| https://cmp.inmobi.com/  | X3/v.java  |
| https://cmp.inmobi.com/  | X3/x.java  |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings  | G0/g.java  |
| https://api.cmp.inmobi.com/  | T3/g.java  |
| http://whatwg.org/html/common-microsyntaxes.html  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/html/webappapis.html  | com/mbridge/msdk/c/b/b.java  |
| https://gist.github.com/atk/1020396\n  | com/mbridge/msdk/c/b/b.java  |
| http://whatwg.org/C  | com/mbridge/msdk/c/b/b.java  |
| https://play.google.com/  | com/mbridge/msdk/click/c.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/click/c.java  |
| https://play.google.com/  | com/mbridge/msdk/click/a.java  |
| https://play.google.com/  | com/mbridge/msdk/foundation/tools/aj.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/tools/aj.java  |
| https://play.google.com/store/apps/details?id=  | com/mbridge/msdk/foundation/webview/a.java  |
| https://play.google.com  | com/mbridge/msdk/mbsignalcommon/windvane/WindVaneWebView.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | com/mbridge/msdk/playercommon/exoplayer2/drm/HttpMediaDrmCallback.java  |
| https://uptodown-android.uptodown.com/android  | com/uptodown/activities/MainActivity.java  |
| https://dw.uptodown.com/dwn/  | com/uptodown/activities/MainActivity.java  |
| https://firebase.google.com/docs/crashlytics/get-started?platform=android  | y0/C2635x.java  |
| https://www.uptodown.app:443  | u2/r.java  |
| https://www.uptodown.com:443  | u2/r.java  |
| https://t.uptodown.app:443  | u2/r.java  |
| https://u.uptodown.app:443  | u2/r.java  |
| https://m.uptodown.net/matomo.php  | u2/C2437A.java  |
| https://www.uptodown.com/turbo?platform=android  | u2/O.java  |
| https://adservice.google.com/getconfig/pubvendors  | u2/O.java  |
| https://www.virustotal.com/gui/file/  | u2/C2453m.java  |
| https://play.google.com  | u2/q.java  |
| http://play.google.com  | u2/q.java  |
| https://secure.uptodown.com:443  | l2/C2065a.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | C/b.java  |
| https://www.youtube.com  | E1/a.java  |
| https://secure.uptodown.com  | m2/C2106a.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | J/y.java  |
| this@installeractivity.packageman  | com/uptodown/core/activities/InstallerActivity.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18222222222  | com/uptodown/activities/MoreInfo.java  |

## **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=ES, ST=Málaga, L=Málaga, O=Uptodown, OU=Uptodown, CN=Uptodown Technologies SL 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-02 15:16:15+00:00 有效期至: 2051-09-18 15:16:15+00:00 发行人: C=ES, ST=Málaga, L=Málaga, O=Uptodown, OU=Uptodown, CN=Uptodown Technologies SL 序列号: 0x4976173c 哈希算法: sha256 md5值: ed86b3c7d53cba96769d1b431108e398 sha1值: 4b64559bc35829fd427bf65985ffdd9a88909fc4 sha256值: 822b9ca12b534ebcf426632221d951bfc60eb08f9f0cf2839c321b0685c2e8a4 sha512值: 45efe48cdaf6f380cb874193acd01d5469ef7fe38e338455817694b3c4d635c16228bd25bb02bb5a402888c35415f165d094888c827709826397def703b2a9ab 公钥算法: rsa 密钥长度: 2048 指纹: 051d3f50665ccdf9ecda376f1c8051d410ef4312c7e745f16fb6d4d0ddebfbc9**

## **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.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.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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.GET\_PACKAGE\_SIZE | 正常 | 测量应用程序存储空间 | 允许应用程序找出任何包使用的空间 |
| 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.USE\_CREDENTIALS | 危险 | 使用帐户的身份验证凭据 | 允许应用程序请求身份验证令牌 |
| android.permission.AUTHENTICATE\_ACCOUNTS | 危险 | 充当帐户验证器 | 允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码 |
| android.permission.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| 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.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.REQUEST\_DELETE\_PACKAGES | 正常 |  | 允许应用程序请求删除包 |
| 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.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.UPDATE\_PACKAGES\_WITHOUT\_USER\_ACTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ENFORCE\_UPDATE\_OWNERSHIP | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| android.permission.DELETE\_PACKAGES | 系统需要 | 删除应用程序 | 允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序 |
| android.permission.ACCESS\_SUPERUSER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.uptodown.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.uptodown.activities.MainActivity | **Schemes**: https://, utd://, market://, http://, content://, file://, \*://, package://, **Hosts:** www.uptodown.com, market.android.com, play.google.com, dw.uptodown.com, \*, **Mime Types:** \*/\*, application/xapk-package-archive, application/vnd.xapk, application/\*, application/apkm-package-archive, application/vnd.apkm, application/apks-package-archive, application/vnd.apks, application/vnd.android.package-archive, **Path Prefixes:** /preregister-available, /dwn, **Path Patterns:** .\*.xapk, .\*..\*.xapk, .\*..\*..\*.xapk, .\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.xapk, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.xapk, .\*.apkm, .\*..\*.apkm, .\*..\*..\*.apkm, .\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apkm, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apkm, .\*.apks, .\*..\*.apks, .\*..\*..\*.apks, .\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apks, .\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*..\*.apks,  |

**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。**