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

**智能K歌（ 2.17.48.2505081546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 | 智能K歌 |
| 版本 | 2.17.48.2505081546 |
| 包名 | com.huiaichang.sdm.desktop |
| 域名线索 | 74条 |
| URL线索 | 66条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | mad-2.17.48.2505081546.sdm.ott.apk |
| 文件大小 | 70.51MB |
| MD5值 | cf21132844dda0ad29d731f458f26884 |
| SHA1值 | b5c3f74b7c1b369379356baceb3743f3dcbc947c |
| SHA256值 | e4ffff79433f68fc860d9bbf673771f93b74324acf5575f81fe146b299fface5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 智能K歌 |
| 包名 | com.huiaichang.sdm.desktop |
| 主活动Activity | com.hhc.muse.desktop.MainActivity |
| 安卓版本名称 | 2.17.48.2505081546 |
| 安卓版本 | 21748 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| pyyaml.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 117.121.4.242 | IP: 117.121.4.242 所属国家: China 地区: Beijing 城市: Beijing  |
| www.satip.info | IP: 35.214.201.169 所属国家: Netherlands 地区: Groningen 城市: Groningen  |
| www.videolan.org | IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris  |
| 192.168.1.201 | IP: 192.168.1.201 所属国家: - 地区: - 城市: -  |
| www.twolame.org | IP: 93.93.131.3 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Cambridge  |
| open.account.preview.n.xiaomi.nethttps | 没有服务器地理信息.  |
| hdns.openspeech.cn | IP: 101.200.180.128 所属国家: China 地区: Beijing 城市: Beijing  |
| lame.sf.net32bitserror | 没有服务器地理信息.  |
| download.cherryonline.cn | IP: 120.79.46.211 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| conn.origjoy.com | IP: 106.75.24.153 所属国家: China 地区: Shanghai 城市: Shanghai  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| logging.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| android.bugly.qq.com | IP: 124.95.225.146 所属国家: China 地区: Liaoning 城市: Shenyang  |
| account.xiaomi.com | IP: 111.202.1.104 所属国家: China 地区: Beijing 城市: Beijing  |
| logs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| musicbrainz.org | IP: 142.132.240.1 所属国家: Germany 地区: Sachsen 城市: Falkenstein  |
| www.twolame.orgmpeg-2 | 没有服务器地理信息.  |
| open.account.preview.n.xiaomi.net | IP: 10.38.161.65 所属国家: - 地区: - 城市: -  |
| mwx.cherryonline.cn | IP: 47.106.99.165 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| api-preview.ai.xiaomi.com | IP: 111.206.101.224 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| log.ktvdaren.com | IP: 106.75.13.136 所属国家: China 地区: Shanghai 城市: Shanghai  |
| log.iflytek.com | IP: 103.8.33.178 所属国家: China 地区: Anhui 城市: Hefei  |
| www.bouncycastle.org | IP: 43.250.142.130 所属国家: Australia 地区: Queensland 城市: Warren  |
| www.oasis-open.org | IP: 172.99.100.168 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| fingerprint.videolan.org | IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris  |
| www.tvdr.de | IP: 88.198.76.220 所属国家: Germany 地区: Bayern 城市: Gunzenhausen  |
| standards.iso.org | IP: 138.81.131.111 所属国家: Switzerland 地区: Geneve 城市: Geneva  |
| www.shoutcast.com | IP: 52.175.64.109 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| relaxng.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| p.ktvsky.com | IP: 106.75.49.43 所属国家: China 地区: Shanghai 城市: Shanghai  |
| aiui.openspeech.cn | IP: 124.243.239.171 所属国家: China 地区: Beijing 城市: Beijing  |
| kcloud.v2.service.ktvdaren.com | IP: 106.75.7.48 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.baidu.com | IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding  |
| m.ktvsky.com | IP: 117.50.16.243 所属国家: China 地区: Shanghai 城市: Shanghai  |
| aiui-ipv6.openspeech.cn | IP: 124.243.239.171 所属国家: China 地区: Beijing 城市: Beijing  |
| mconno.cherryonline.cn | IP: 47.106.99.165 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| lame.sf.net | IP: 104.18.21.237 所属国家: United States of America 地区: California 城市: San Francisco  |
| bridge.io.mi.com | IP: 111.202.1.75 所属国家: China 地区: Beijing 城市: Beijing  |
| musicopen.console.ktvdaren.com | IP: 106.75.56.78 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mconn.cherryonline.cn | IP: 39.108.124.38 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| judaikeji.cn | IP: 47.99.43.47 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.shoutcast.coms | 没有服务器地理信息.  |
| rqd.uu.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| account-staging.ai.xiaomi.com | 没有服务器地理信息.  |
| open.music.ktvdaren.com | IP: 106.75.24.153 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.xmlsoap.org | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| account.ai.xiaomi.com | IP: 124.251.100.45 所属国家: China 地区: Beijing 城市: Beijing  |
| api.ai.xiaomi.com | IP: 123.125.102.163 所属国家: China 地区: Beijing 城市: Beijing  |
| schemas.upnp.org | 没有服务器地理信息.  |
| account.preview.n.xiaomi.net | IP: 10.38.161.65 所属国家: - 地区: - 城市: -  |
| www.broadcom.com | IP: 104.18.37.111 所属国家: United States of America 地区: California 城市: San Francisco  |
| coupon.stage.ktvsky.com | IP: 106.75.50.247 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.ffmpeg.org | IP: 79.124.17.100 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| hbeat.ktvsky.com | IP: 106.75.33.131 所属国家: China 地区: Shanghai 城市: Shanghai  |
| api-staging.ai.xiaomi.com | 没有服务器地理信息.  |
| uc.qbox.me | IP: 153.99.246.133 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| coupon.ktvsky.com | IP: 106.75.104.202 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.icecast.org | IP: 140.211.166.31 所属国家: United States of America 地区: Oregon 城市: Eugene  |
| restapi.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| musicbrainz.orgtxxxtracktotalmusicbrainz | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.brynosaurus.com | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| apilocate.amap.com | IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing  |
| android.googlesource.com | IP: 142.251.188.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| uplog.qbox.me | IP: 153.99.246.132 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| pub.cdn.cherryonline.cn | IP: 163.177.221.145 所属国家: China 地区: Guangdong 城市: Dongguan  |
| account-staging.ai.xiaomi.comhttps | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| open.account.xiaomi.com | IP: 123.125.102.111 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | com/hhc/muse/desktop/bwu.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | com/hhc/muse/desktop/bww.java  |
| http://%s  | com/hhc/muse/desktop/bsp.java  |
| http://schemas.android.com/apk/res/android  | com/hhc/muse/desktop/bs.java  |
| https://judaikeji.cn/charge\_sys/app/  | com/hhc/muse/desktop/rc.java  |
| https://conn.origjoy.com  | com/hhc/muse/desktop/adn.java  |
| https://account.ai.xiaomi.com  | com/hhc/muse/desktop/axq.java  |
| http://www.slf4j.org/codes.html  | com/hhc/muse/desktop/cxh.java  |
| http://download.cherryonline.cn/release/muse/sgsrf\_7.4.1048\_dangbei.apk  | com/hhc/muse/desktop/amx.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/hhc/muse/desktop/rp.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/hhc/muse/desktop/rp.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/hhc/muse/desktop/rp.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/hhc/muse/desktop/rw.java  |
| http://%s:%d/%s  | com/hhc/muse/desktop/rw.java  |
| https://uc.qbox.me  | com/hhc/muse/desktop/bsn.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/hhc/muse/desktop/bvo.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/hhc/muse/desktop/bvv.java  |
| https://mwx.cherryonline.cn/mv/oa?b=  | com/hhc/muse/desktop/azg.java  |
| https://mconn.cherryonline.cn  | com/hhc/muse/desktop/azg.java  |
| https://mconno.cherryonline.cn  | com/hhc/muse/desktop/azg.java  |
| https://mwx.cherryonline.cn/c/active/  | com/hhc/muse/desktop/azg.java  |
| https://mwx.cherryonline.cn/c/recharge/  | com/hhc/muse/desktop/azg.java  |
| https://mwx.cherryonline.cn/store/r?b=  | com/hhc/muse/desktop/azg.java  |
| http://%s:%d/%s  | com/hhc/muse/desktop/rn.java  |
| https://pub.cdn.cherryonline.cn/  | com/hhc/muse/desktop/ayg.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | com/hhc/muse/desktop/bwa.java  |
| https://uplog.qbox.me/log/3  | com/hhc/muse/desktop/bsm.java  |
| https://account.ai.xiaomi.com  | com/hhc/muse/desktop/bga.java  |
| http://aiui-ipv6.openspeech.cn  | com/hhc/muse/desktop/bga.java  |
| http://pyyaml.org/wiki/YAMLColonInFlowContext  | com/hhc/muse/desktop/dai.java  |
| https://account.ai.xiaomi.com/thirdparty/auth/token  | com/hhc/muse/desktop/feature/ai/d.java  |
| https://conn.origjoy.com  | com/hhc/muse/desktop/network/domain/DomainParserController.java  |
| http://restapi.amap.com  | com/iflytek/aiui/pro/n.java  |
| http://apilocate.amap.com/mobile/sdkchannel  | com/iflytek/aiui/pro/g.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/iflytek/aiui/pro/j.java  |
| http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s  | com/iflytek/aiui/pro/ac.java  |
| https://github.com/yyued/SVGAPlayer-Android  | com/opensource/svgaplayer/h.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://www.baidu.com  | com/thunder/android/stb/util/http/HttpDownloadHelper.java  |
| http://coupon.stage.ktvsky.com/  | com/thunder/android/stb/util/http/HttpDownloadHelper.java  |
| http://hbeat.ktvsky.com/whoami  | com/thunder/ktv/o3.java  |
| http://kcloud.v2.service.ktvdaren.com  | com/thunder/ktv/player/helper/LyricsHelper.java  |
| http://log.ktvdaren.com/logs/vod\_down  | com/thunder/ktv/player/mediaplayer/video/SongDownloader.java  |
| https://coupon.ktvsky.com/stb/mac/login?mac\_id=  | com/thunder/ktv/player/service/b.java  |
| http://m.ktvsky.com/stb1/qr/oem/v2  | com/thunder/ktv/thunderextension/tvlayer/operateqrcode/a.java  |
| http://192.168.1.201/video/disk-07/music\_28/7020128.ts  | com/thunder/ktv/thunderstream/a.java  |
| https://kcloud.v2.service.ktvdaren.com/  | com/thunder/miaimedia/GlobalConfig.java  |
| https://api-preview.ai.xiaomi.com  | com/thunder/miaimedia/MiSigUtils.java  |
| https://account.ai.xiaomi.com/  | com/thunder/miaimedia/security/MiSecurityManager.java  |
| https://bridge.io.mi.com  | com/thunder/miaimedia/security/MiSecurityManager.java  |
| http://coupon.stage.ktvsky.com/  | com/thunder/miaimedia/utils/HttpDownloadHelper.java  |
| http://account.preview.n.xiaomi.net  | com/xiaomi/account/openauth/XiaomiOAuthConstants.java  |
| https://account.xiaomi.com  | com/xiaomi/account/openauth/XiaomiOAuthConstants.java  |
| http://open.account.preview.n.xiaomi.net  | com/xiaomi/account/openauth/XiaomiOAuthConstants.java  |
| https://open.account.xiaomi.com  | com/xiaomi/account/openauth/XiaomiOAuthConstants.java  |
| https://api.ai.xiaomi.com/track/v2  | com/xiaomi/ai/utils/k.java  |
| https://api-preview.ai.xiaomi.com/track/v2  | com/xiaomi/ai/utils/k.java  |
| https://api.ai.xiaomi.com/track/authmiot  | com/xiaomi/ai/utils/k.java  |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |
| http://www.bouncycastle.org  | 摸瓜V3引擎  |
| https://aiui-ipv6.openspeech.cn:443/v1.1/server/register  | 摸瓜V3引擎  |
| https://account.ai.xiaomi.com/  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://www.brynosaurus.com/cachedir/  | 摸瓜V3引擎  |
| http://www.icecast.org/  | 摸瓜V3引擎  |
| http://www.videolan.org/x264.html  | 摸瓜V3引擎  |
| http://www.broadcom.com/licenses/LGPLv2.1.php  | 摸瓜V3引擎  |
| https://github.com/google/gson/blob/main/Troubleshooting.md#  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/envelope/Body  | 摸瓜V3引擎  |
| http://hbeat.ktvsky.com/whoami  | 摸瓜V3引擎  |
| http://apilocate.amap.com/mobile/sdkchannel  | 摸瓜V3引擎  |
| http://www.videolan.org  | 摸瓜V3引擎  |
| http://www.satip.info/Playlists/%s.m3u  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android22skin.support.constraint.SkinCompatConstraintLayout  | 摸瓜V3引擎  |
| http://www.videolan.org/vlc/playlist/0  | 摸瓜V3引擎  |
| http://api-staging.ai.xiaomi.com/track/perf  | 摸瓜V3引擎  |
| http://www.shoutcast.com%s?id=%s  | 摸瓜V3引擎  |
| http://coupon.stage.ktvsky.com/  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | 摸瓜V3引擎  |
| http://www.satip.info/Playlists/%s.m3uremoveServerRemoving  | 摸瓜V3引擎  |
| https://coupon.ktvsky.com/stb/mac/login?mac\_id=  | 摸瓜V3引擎  |
| https://account.ai.xiaomi.com  | 摸瓜V3引擎  |
| http://logging.apache.org/log4j/2.x/manual/configuration.html#ConfigurationSyntax  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com/track/perfhttps://api.ai.xiaomi.com/track/perfhttp://api-staging.a  | 摸瓜V3引擎  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtdENTITY  | 摸瓜V3引擎  |
| https://kcloud.v2.service.ktvdaren.com/  | 摸瓜V3引擎  |
| http://www.baidu.com  | 摸瓜V3引擎  |
| http://https://uclibavformat/hls.cBANDWIDTH=AUDIO=VIDEO=SUBTITLES=METHOD=URI=IV=TYPE=GROUP-ID=LANGUA  | 摸瓜V3引擎  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | 摸瓜V3引擎  |
| http://lame.sf.net  | 摸瓜V3引擎  |
| http://relaxng.org/ns/structure/1.0  | 摸瓜V3引擎  |
| http://musicbrainz.orgTXXXTRACKTOTALMusicBrainz  | 摸瓜V3引擎  |
| http://restapi.amap.com  | 摸瓜V3引擎  |
| https://restapi.amap.com/v3/iasdkauth  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/track/authmiot  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/track/v2  | 摸瓜V3引擎  |
| https://bridge.io.mi.com  | 摸瓜V3引擎  |
| https://open.account.xiaomi.com  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/encoding/  | 摸瓜V3引擎  |
| http://m.ktvsky.com/stb1/qr/oem/v2  | 摸瓜V3引擎  |
| http://www.twolame.org  | 摸瓜V3引擎  |
| https://github.com/yyued/SVGAPlayer-Android#cache  | 摸瓜V3引擎  |
| http://schemas.upnp.org/upnp/1/0/  | 摸瓜V3引擎  |
| http://account.preview.n.xiaomi.net  | 摸瓜V3引擎  |
| https://conn.origjoy.com  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%shttps://api.ai.xiaomi  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com/track/v2  | 摸瓜V3引擎  |
| https://account.xiaomi.com  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/envelope/  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com/track/perf  | 摸瓜V3引擎  |
| https://fingerprint.videolan.org/acoustid.php?meta=recordings  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/track/v1  | 摸瓜V3引擎  |
| http://logging.apache.org/log4j/1.2/faq.html#unload.  | 摸瓜V3引擎  |
| https://account.ai.xiaomi.com/thirdparty/auth/token  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| http://www.tvdr.de/).  | 摸瓜V3引擎  |
| http://logging.apache.org/log4j/2.0/events  | 摸瓜V3引擎  |
| http://192.168.1.201/video/disk-07/music\_28/7020128.ts  | 摸瓜V3引擎  |
| http://account-staging.ai.xiaomi.com  | 摸瓜V3引擎  |
| http://kcloud.v2.service.ktvdaren.com  | 摸瓜V3引擎  |
| http://standards.iso.org/ittf/PubliclyAvailableStandards/MPEG-DASH\_schema\_files/DASH-MPD.xsd  | 摸瓜V3引擎  |
| http://www.shoutcast.com/sbin/newxml.phtml?genre=%s  | 摸瓜V3引擎  |
| http://www.twolame.orgMPEG-2  | 摸瓜V3引擎  |
| http://account-staging.ai.xiaomi.comhttps://account.ai.xiaomi.comapp\_tokenmiBrainSdkAnonymousOauthRe  | 摸瓜V3引擎  |
| http://www.shoutcast.com/sbin/tunein-tvstation.pls?id=%s  | 摸瓜V3引擎  |
| http://www.icecast.org/x-audiocast-genre:  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/track/perf  | 摸瓜V3引擎  |
| https://api-preview.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | 摸瓜V3引擎  |
| http://logging.apache.org/log4j/1.2/faq.html#noconfig  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://open.account.preview.n.xiaomi.nethttps://account.xiaomi.commibrain\_oauth\_getreflesh\_token  | 摸瓜V3引擎  |
| http://lame.sf.net32bitsError:  | 摸瓜V3引擎  |
| http://open.account.preview.n.xiaomi.net  | 摸瓜V3引擎  |
| http://www.videolan.org/vlc  | 摸瓜V3引擎  |
| https://api.ai.xiaomi.com/track/authmiothttps://api.ai.xiaomi.com/track/v1aivs\_post\_trackmsg  | 摸瓜V3引擎  |
| http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s  | 摸瓜V3引擎  |
| http://api-staging.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | 摸瓜V3引擎  |
| http://log.ktvdaren.com/logs/vod\_down  | 摸瓜V3引擎  |
| http://relaxng.org/ns/structure/1.0validating  | 摸瓜V3引擎  |
| http://musicbrainz.org  | 摸瓜V3引擎  |
| http://www.tvdr.de/).VDR  | 摸瓜V3引擎  |
| http://aiui.openspeech.cn:80/aiui/v1/pushnode.do  | lib/armeabi-v7a/libaiui.so  |
| http://117.121.4.242:3200  | lib/armeabi-v7a/libaiui.so  |
| https://aiui.openspeech.cn:443/v1.1/server/register  | lib/armeabi-v7a/libaiui.so  |
| https://aiui.openspeech.cn:443/athena/opsync  | lib/armeabi-v7a/libaiui.so  |
| https://aiui.openspeech.cn/athena/instant  | lib/armeabi-v7a/libaiui.so  |
| https://log.iflytek.com:443/log  | lib/armeabi-v7a/libaiui.so  |
| http://hdns.openspeech.cn:80/sip/resolver  | lib/armeabi-v7a/libaiui.so  |
| http://aiui.openspeech.cn:80/sync/v1/upload.do  | lib/armeabi-v7a/libaiui.so  |
| http://aiui.openspeech.cn:80/sync/v1/syncthird.do  | lib/armeabi-v7a/libaiui.so  |
| http://%s:8150/mls-api/v1/local-song/get-pageignore  | lib/armeabi-v7a/libgojni.so  |
| http://127.0.0.1:9090/hlwproxy?ts=%d&appid=%s&cid=%s&token=%s  | lib/armeabi-v7a/libhlw.so  |
| https://api-preview.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://api.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | lib/armeabi-v7a/libmibrainsdk.so  |
| http://api-staging.ai.xiaomi.com/cp\_resource\_locator/c/v1.0/provider/%s/ids/%s  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://api.ai.xiaomi.com/track/authmiot  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://api.ai.xiaomi.com/track/v1  | lib/armeabi-v7a/libmibrainsdk.so  |
| http://open.account.preview.n.xiaomi.net  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://account.xiaomi.com  | lib/armeabi-v7a/libmibrainsdk.so  |
| http://account-staging.ai.xiaomi.com  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://account.ai.xiaomi.com  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://api-preview.ai.xiaomi.com/track/perf  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://api.ai.xiaomi.com/track/perf  | lib/armeabi-v7a/libmibrainsdk.so  |
| http://api-staging.ai.xiaomi.com/track/perf  | lib/armeabi-v7a/libmibrainsdk.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/armeabi-v7a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libmobileffmpeg.so  |
| http://%s:%d  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.satip.info/Playlists/%s.m3u  | lib/armeabi-v7a/libmusicplayer.so  |
| http://musicbrainz.org  | lib/armeabi-v7a/libmusicplayer.so  |
| http://location  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.shoutcast.com/sbin/newxml.phtml?genre=%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.shoutcast.com/sbin/tunein-tvstation.pls?id=%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.shoutcast.com%s?id=%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.videolan.org/vlc/playlist/0  | lib/armeabi-v7a/libmusicplayer.so  |
| http://%s:8008%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://%s%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://%s:%d%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.tvdr.de/).  | lib/armeabi-v7a/libmusicplayer.so  |
| https://fingerprint.videolan.org/acoustid.php?meta=recordings+tracks+usermeta+releases&duration=%d&fingerprint=%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.videolan.org/vlc  | lib/armeabi-v7a/libmusicplayer.so  |
| http://%s%s%s  | lib/armeabi-v7a/libmusicplayer.so  |
| http://lame.sf.net  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/armeabi-v7a/libmusicplayer.so  |
| http://relaxng.org/ns/structure/1.0  | lib/armeabi-v7a/libmusicplayer.so  |
| http://schemas.xmlsoap.org/soap/envelope/  | lib/armeabi-v7a/libmusicplayer.so  |
| http://[  | lib/armeabi-v7a/libmusicplayer.so  |
| http://schemas.upnp.org/upnp/1/0/  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.icecast.org/  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.twolame.org  | lib/armeabi-v7a/libmusicplayer.so  |
| http://www.videolan.org/x264.html  | lib/armeabi-v7a/libmusicplayer.so  |
| http://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libmusicplayer.so  |
| https://musicopen.console.ktvdaren.com  | lib/armeabi-v7a/libplayerjni.so  |
| https://p.ktvsky.com  | lib/armeabi-v7a/libplayerjni.so  |
| https://conn.origjoy.com  | lib/armeabi-v7a/libplayerjni.so  |
| https://open.music.ktvdaren.com  | lib/armeabi-v7a/libplayerjni.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/hhc/muse/desktop/rp.java  |
| your.account@domain.com  | org/acra/sender/DefaultReportSenderFactory.java  |
| jxwang@iflytek.com  | lib/armeabi-v7a/libhlw.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |
| info@underbit.com  | lib/armeabi-v7a/libmibraindec.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libmobileffmpeg.so  |
| sam@zoy.org libdvbpsi-devel@videolan.org fsync@openssh.com fstatvfs@openssh.com statvfs@openssh.com hmac-ripemd160@openssh.com zlib@openssh.com rijndael-cbc@lysator.liu twolame-discuss@lists.sourceforg keepalive@libssh2.orgw  | lib/armeabi-v7a/libmusicplayer.so  |
| ftp@example.com  | lib/armeabi-v7a/libplayerjni.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |
| 14389071831  | lib/armeabi-v7a/libmusicplayer.so  |

## **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: ST=gd, L=gz, O=og, OU=og, CN=og 签名算法: rsassa\_pkcs1v15 有效期自: 2021-06-16 08:21:11+00:00 有效期至: 2121-05-23 08:21:11+00:00 发行人: ST=gd, L=gz, O=og, OU=og, CN=og 序列号: 0x3443545f 哈希算法: sha256 md5值: fac84329de2b62afd3ebdd8b2cf4a43a sha1值: 0109f097bf33533dfda23df2e731922fcdfc2ae9 sha256值: fc035c52f544c5148be895c56de91b9ed17512bf53ef79876d9c2f5897a95f1c sha512值: 0c39821ffe81d383338acc5f54ed1454fbc9535778d3cdc5f804afc9f6077537d68419af441bb8ca04c77e206bc5f53ed2aaa940b3110868c8659870c162367b 公钥算法: rsa 密钥长度: 2048 指纹: e355109eea402ad78fcc861926343b795251521e91bb8907e3c1386fa01f6328**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "code\_authorized\_expired" : "服务器授权已过期"  |
| "code\_get\_download\_url\_err\_auth" : "获取下载链接失败，请检查网络"  |
| "code\_place\_no\_auth" : "非场所管理员, 无权限访问"  |
| "info\_mi\_token" : "小爱Token：%1$s"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "pwd\_forbidden" : "您已多次输入密码错误，无法继续尝试！"  |
| "setting\_auth\_storage" : "硬盘读写权限"  |
| "setting\_auth\_storage\_fail" : "开启读写权限失败！%1$s"  |
| "setting\_auth\_storage\_loading" : "开启读写权限中……"  |
| "setting\_auth\_storage\_repair" : "去修复"  |
| "setting\_auth\_storage\_success" : "开启读写权限成功，应用即将自动重启！"  |
| "setting\_need\_pwd" : "设置密码(542317)"  |
| "setting\_need\_pwd\_tip" : "开启设置密码后，进入设置时需要输入密码：542317"  |
| "setting\_power\_need\_pwd" : "关机和重启密码(542317)"  |
| "wifi\_pwd" : "Wi-Fi密码："  |
| "code\_authorized\_expired" : "การให้สิทธิ์เซิร์ฟเวอร์หมดอายุ"  |
| "code\_get\_download\_url\_err\_auth" : "ล้มเหลวที่จะได้รับการดาวน์โหลด URL เนื่องจากการรับรองความถูกต้องทำบาป"  |
| "code\_place\_no\_auth" : "ล้มเหลวในการเข้าถึงโดยไม่มีอำนาจ"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "Ủy quyền máy chủ đã hết hạn"  |
| "code\_get\_download\_url\_err\_auth" : "Không thể có được tải về url, vì auth err"  |
| "code\_place\_no\_auth" : "Không thể truy cập mà không có thẩm quyền"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "Bạn đã nhập sai mật khẩu quá nhiều lần, tài khoản đã bị đóng băng！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Đặt mật khẩu(542317)"  |
| "setting\_need\_pwd\_tip" : "nếu bạn bật cài đặt mật khẩu ， bạn cần nhập mật khẩu ： 542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "Nag-expire na ang pahintulot ng server"  |
| "code\_get\_download\_url\_err\_auth" : "Nabigong kunin download url, dahil sa err auth"  |
| "code\_place\_no\_auth" : "Nabigong i-access nang walang awtoridad"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "Mayroon kang maling maling pag-input ng maraming beses, ang account ay na-freeze！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Itakda ang password(542317)"  |
| "setting\_need\_pwd\_tip" : "Kung pinagana mo ang setting ng password, kailangan mo ng input password ： 542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "ការអនុញ្ញាតម៉ាស៊ីនមេបានផុតកំណត់ហើយ"  |
| "code\_get\_download\_url\_err\_auth" : "获取下载链接失败，请检查网络"  |
| "code\_place\_no\_auth" : "អ្នកគ្រប់គ្រងមិនមែនកន្លែងគ្មានសិទ្ធិក្នុងការទស្សនាទេ"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "Server authorization has expired"  |
| "code\_get\_download\_url\_err\_auth" : "Failed to get download url, because of the err auth"  |
| "code\_place\_no\_auth" : "Failed to access without authority"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "setting\_power\_need\_pwd" : "Power off and reboot password(542317)"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "ການອະນຸຍາດຂອງເຊີບເວີ ໝົດ ອາຍຸແລ້ວ"  |
| "code\_get\_download\_url\_err\_auth" : "获取下载链接失败，请检查网络"  |
| "code\_place\_no\_auth" : "ຜູ້ບໍລິຫານທີ່ບໍ່ແມ່ນສະຖານທີ່, ບໍ່ມີສິດທີ່ຈະໄປຢ້ຽມຢາມ"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "Kebenaran pelayan telah tamat"  |
| "code\_get\_download\_url\_err\_auth" : "Gagal untuk mendapatkan muat turun url, kerana auth sesat yang"  |
| "code\_place\_no\_auth" : "Gagal akses tanpa kuasa"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "ဆာဗာခွင့်ပြုချက်သက်တမ်းကုန်သွားပြီ"  |
| "code\_get\_download\_url\_err\_auth" : "获取下载链接失败，请检查网络"  |
| "code\_place\_no\_auth" : "非场所管理员, 无权限访问"  |
| "info\_mi\_token" : "Ai Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "Otorisasi server telah kedaluwarsa"  |
| "code\_get\_download\_url\_err\_auth" : "Gagal mendapatkan url download, karena auth err"  |
| "code\_place\_no\_auth" : "Gagal akses tanpa otoritas"  |
| "info\_mi\_token" : "小爱Token：%1$s"  |
| "pwd\_forbidden" : "You have input wrong password too many times, account has been frozen！"  |
| "setting\_auth\_storage" : "Disk storage Permission"  |
| "setting\_auth\_storage\_fail" : "Authorize permission fail! %1$s"  |
| "setting\_auth\_storage\_loading" : "Authorizing......"  |
| "setting\_auth\_storage\_repair" : "Go Fix It"  |
| "setting\_auth\_storage\_success" : "Authorize success, app will restart now!"  |
| "setting\_need\_pwd" : "Setting password(542317)"  |
| "setting\_need\_pwd\_tip" : "if you enable setting password，you need input password：542317"  |
| "wifi\_pwd" : "Wi-Fi Password："  |
| "code\_authorized\_expired" : "服務器授權已過期"  |
| "code\_get\_download\_url\_err\_auth" : "獲取下載鏈接失敗，請檢查網絡"  |
| "code\_place\_no\_auth" : "非場所管理員, 無權限訪問"  |
| "info\_mi\_token" : "小爱Token：%1$s"  |
| "pwd\_forbidden" : "多次輸入密碼錯誤，無法繼續嘗試！"  |
| "setting\_auth\_storage" : "硬盤讀寫權限"  |
| "setting\_auth\_storage\_fail" : "開啟讀寫權限失敗！%1$s"  |
| "setting\_auth\_storage\_loading" : "開啟讀寫權限中……"  |
| "setting\_auth\_storage\_repair" : "去修復"  |
| "setting\_auth\_storage\_success" : "開啟讀寫權限成功，應用即將自動重啟！"  |
| "setting\_need\_pwd" : "設置密碼(542317)"  |
| "setting\_need\_pwd\_tip" : "開啟設置密碼後，進入設置時需要輸入密碼：542317"  |
| "setting\_power\_need\_pwd" : "關機和重啟密碼(542317)"  |
| "wifi\_pwd" : "Wi-Fi密碼："  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.SET\_TIME | 系统需要 | 设定时间 | 允许应用程序更改手机的时钟时间 |
| android.permission.SET\_TIME\_ZONE | 系统需要 | 设置时区 | 允许应用程序更改手机的时区 |
| 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.WRITE\_MEDIA\_STORAGE | 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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.DELETE\_CACHE\_FILES | 系统需要 | 删除其他应用程序缓存 | 允许应用程序删除缓存文件 |
| android.permission.CLEAR\_APP\_CACHE | 系统需要 | 删除所有应用程序缓存数据 | 允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。  |
| android.permission.HI\_SYSTEM\_MANAGER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |

## **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。**