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

**糖心Vlog（ 4.6.0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 | 糖心Vlog |
| 版本 | 4.6.0 |
| 包名 | com.flutter324.ctnnx.lr0e8w |
| 域名线索 | 51条 |
| URL线索 | 27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 | 20250705-043013.apk |
| 文件大小 | 57.21MB |
| MD5值 | 987fb490d5bcca385caed4d14d7884d5 |
| SHA1值 | 01d7d75930a08544ba318edb4289944ed6128334 |
| SHA256值 | 82340912bacd12af14d7adcd3fff69816be2d0ccfbb0ced2e8940ad06f92db0a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 糖心Vlog |
| 包名 | com.flutter324.ctnnx.lr0e8w |
| 主活动Activity | com.example.flutter3\_frame.MainActivity |
| 安卓版本名称 | 4.6.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api-txvlog.uxavma85y8.com | IP: 104.21.16.160 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.tensorflow.org | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| jajgjw.ijingrui.org.8407c35e.cdnhwcaoc115.cn | 没有服务器地理信息.  |
| a.app.qq.com | IP: 60.28.219.32 所属国家: China 地区: Tianjin 城市: Tianjin  |
| dashif.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| jsoup.org | IP: 104.21.112.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| 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.qq.com | IP: 221.198.70.47 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.example.com | IP: 23.193.186.17 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| jajgjw.ijingrui.org | 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  |
| html.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| hcdnd101.sme.foreign.cdnhwcaoc115.cn | IP: 106.74.32.242 所属国家: China 地区: Shandong 城市: Jinan  |
| aomedia.org | IP: 74.86.151.167 所属国家: United States of America 地区: California 城市: San Jose  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| android.googlesource.com | IP: 74.125.20.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.xgxjg72vl7.com | IP: 3.169.183.54 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.webrtc.org | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.google.com | IP: 31.13.94.41 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| streams.videolan.org | IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris  |
| api.nzc5qxxuzm.com | IP: 3.169.183.5 所属国家: United States of America 地区: Washington 城市: Seattle  |
| dts5zlpcs45kz.cloudfront.net | IP: 3.169.183.5 所属国家: United States of America 地区: Washington 城市: Seattle  |
| api-tx.x8qpjon3eh.info | IP: 104.21.85.239 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.mi.com | IP: 221.194.175.44 所属国家: China 地区: Hebei 城市: Langfang  |
| webrtc.googlesource.com | IP: 74.125.195.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| uggfr1242.com | IP: 156.234.51.252 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| developer.apple.com | IP: 92.123.180.26 所属国家: Italy 地区: Lombardia 城市: Milan  |
| fdbndkgaa.xy0buop0.com | IP: 156.234.51.251 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| try.jsoup.org | IP: 104.21.96.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ffmpeg.org | IP: 79.124.17.100 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| play.google.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| plus.google.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| default.url | 没有服务器地理信息.  |
| jajgjw.ijingrui.org.slowdark.com | 没有服务器地理信息.  |
| developer.android.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.ibm.com | IP: 23.1.167.82 所属国家: Japan 地区: Osaka 城市: Ibaraki  |
| txapp.tv | IP: 108.139.10.69 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.lakkagmg6m.com | IP: 3.169.183.114 所属国家: United States of America 地区: Washington 城市: Seattle  |
| api.5fryvs202i.com | IP: 3.169.183.5 所属国家: United States of America 地区: Washington 城市: Seattle  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| api-tx.vf43zauqc7.info | IP: 172.67.203.8 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.za1swxom5t.com | IP: 3.169.183.117 所属国家: United States of America 地区: Washington 城市: Seattle  |
| aomediacodec.github.io | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.microsoft.com | IP: 13.107.246.73 所属国家: United States of America 地区: Washington 城市: Redmond  |
| api.uo3mpfbi5l.com | IP: 3.169.183.114 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| api-txvlog.ku0g6y1ag9.com | IP: 172.67.151.11 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 |
| --- | --- |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| http://dashif.org/guidelines/last-segment-number  | a5/d.java  |
| http://dashif.org/guidelines/trickmode  | a5/d.java  |
| http://dashif.org/thumbnail\_tile  | a5/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | a5/d.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/c.java  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | q5/z.java  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | u3/x0.java  |
| https://play.google.com/store/apps/details?id=  | t2/a.java  |
| http://www.google.com  | t2/a.java  |
| https://a.app.qq.com/o/simple.jsp?pkgname=  | t2/b.java  |
| https://app.mi.com/details?id=  | t2/c.java  |
| https://app.mi.com  | t2/c.java  |
| https://x</LA\_URL>  | y3/k0.java  |
| https://default.url  | y3/k0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | y3/l0.java  |
| http://undefined/  | oc/d.java  |
| https://plus.google.com/  | z5/j1.java  |
| http://ns.adobe.com/xap/1.0/  | e4/a.java  |
| https://aomedia.org/emsg/ID3  | o4/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | o4/a.java  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://webrtc.googlesource.com/src/  | 摸瓜V3引擎  |
| gprticknfp  | 摸瓜V3引擎  |
| jajgjw.ijingrui.org.8407c35e.cdnhwcaoc115.cn  | 摸瓜V3引擎  |
| https://jsoup.org/bugs  | 摸瓜V3引擎  |
| https://crbug.com/1053756  | 摸瓜V3引擎  |
| https://github.com/jhy/jsoup/blob/master/src/main/java/org/jsoup/examples/Wikipedia.java).  | 摸瓜V3引擎  |
| https://jsoup.org/download  | 摸瓜V3引擎  |
| icwhuzdegjl  | 摸瓜V3引擎  |
| https://github.com/jhy/jsoup/actions?query=workflow%3ABuild  | 摸瓜V3引擎  |
| https://default.url  | 摸瓜V3引擎  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | 摸瓜V3引擎  |
| https://jsoup.org/colophon  | 摸瓜V3引擎  |
| https://app.mi.com  | 摸瓜V3引擎  |
| jajgjw.ijingrui.org  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/last-segment-number  | 摸瓜V3引擎  |
| https://jsoup.org/license).  | 摸瓜V3引擎  |
| https://github.com/arthenica/ffmpeg-kit/wiki/Source  | 摸瓜V3引擎  |
| hcdnd101.sme.foreign.cdnhwcaoc115.cn  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/permissions/overview  | 摸瓜V3引擎  |
| https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/thumbnail\_tile  | 摸瓜V3引擎  |
| https://jsoup.org/cookbook/  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| http://www.unicode.org/copyright.html  | 摸瓜V3引擎  |
| https://jsoup.org/cookbook/cleaning-html/safelist-sanitizer  | 摸瓜V3引擎  |
| dts5zlpcs45kz.cloudfront.net  | 摸瓜V3引擎  |
| https://github.com/jhy/jsoup).  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://jsoup.org/cookbook/input/parse-document-from-string  | 摸瓜V3引擎  |
| https://a.app.qq.com/o/simple.jsp?pkgname=  | 摸瓜V3引擎  |
| uggfr1242.com  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted  | 摸瓜V3引擎  |
| https://jsoup.org/cookbook/modifying-data/set-html  | 摸瓜V3引擎  |
| fdbndkgaa.xy0buop0.com  | 摸瓜V3引擎  |
| msqutgepyzxw  | 摸瓜V3引擎  |
| https://github.com/jhy/jsoup/workflows/Build/badge.svg  | 摸瓜V3引擎  |
| https://jsoup.org/cookbook/extracting-data/selector-syntax  | 摸瓜V3引擎  |
| https://github.com/dart-lang/sdk/blob/master/runtime/docs/compiler/aot/entry\_point\_pragma.md  | 摸瓜V3引擎  |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread  | 摸瓜V3引擎  |
| jajgjw.ijingrui.org.slowdark.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://app.mi.com/details?id=  | 摸瓜V3引擎  |
| https://html.spec.whatwg.org/multipage/  | 摸瓜V3引擎  |
| https://github.com/flutter/flutter/issues.  | 摸瓜V3引擎  |
| https://try.jsoup.org/~LGB7rk\_atM2roavV0d-czMt3J\_g  | 摸瓜V3引擎  |
| https://aomedia.org/emsg/ID3  | 摸瓜V3引擎  |
| https://jsoup.org/discussion).  | 摸瓜V3引擎  |
| http://dashif.org/thumbnail\_tile  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/trickmode  | 摸瓜V3引擎  |
| api.uo3mpfbi5l.com  | 摸瓜V3引擎  |
| https://jsoup.org/apidocs/).  | 摸瓜V3引擎  |
| https://jsoup.org/  | 摸瓜V3引擎  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/arm64-v8a/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/arm64-v8a/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/arm64-v8a/libffmpegkit.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://crbug.com/1053756  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/,  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| https://aomediacodec.github.io/av1-rtp-spec/  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| http://api-tx.x8qpjon3eh.info/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://api.nzc5qxxuzm.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| https://txapp.tv  | lib/armeabi-v7a/libapp.so  |
| http://api-txvlog.uxavma85y8.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://api.uo3mpfbi5l.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://api.xgxjg72vl7.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| http://api.lakkagmg6m.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://www.qq.com  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| http://api-tx.vf43zauqc7.info/cxapi  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| http://api.za1swxom5t.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://api.5fryvs202i.com/cxapi  | lib/armeabi-v7a/libapp.so  |
| http://api-txvlog.ku0g6y1ag9.com/cxapi  | 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  |
| http://api.  | lib/armeabi-v7a/libapp.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://http  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libffmpegkit.so  |
| https://streams.videolan.org/upload/  | lib/armeabi-v7a/libffmpegkit.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libffmpegkit.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| https://streams.videolan.org/upload/  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://crbug.com/1053756  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/,  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| https://aomediacodec.github.io/av1-rtp-spec/  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn  | lib/armeabi-v7a/libjingle\_peerconnection\_so.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | w5/q.java  |
| android-sdk-releaser@livw11.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/arm64-v8a/libffmpegkit.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| appro@openssl.org  | lib/arm64-v8a/libjingle\_peerconnection\_so.so  |
| \_httpparser@13463476.responsepa \_hashcollisionnode@642137193.fromcollis \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_compressednode@642137193.single \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_casterror@0150898.\_create \_invocationmirror@0150898.\_withtype velocitytrackermixin@434039605.withkind \_rawsocket@14069316.\_writepipe \_colorfilter@15065589.lineartosr \_uri@0150898.file \_growablelist@0150898.\_literal1 \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of \_nativesocket@14069316.pipe \_cookie@13463476.fromsetcoo linnannan101@gmail.com authenticationscheme@13463476.fromstring \_list@0150898.of \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie storationinformation@1010124995.fromserial \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe \_socket@14069316.\_readpipe \_list@0150898.\_ofother \_bytebuffer@7027147.\_new ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_filestream@14069316.forstdin \_colorfilter@15065589.srgbtoline \_uri@0150898.directory \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.generate \_routedata@1683504625.ofroute \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| android-sdk-releaser@livw11.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libffmpegkit.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libffmpegkit\_armv7a\_neon.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | w6/a.java  |

## **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: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2025-07-04 20:30:05+00:00 有效期至: 2052-11-19 20:30:05+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0x2d419bd9 哈希算法: sha256 md5值: a0674dd9cc04f2ff5e64b0feee33e9cd sha1值: cb350f645f2ff464c1f6f466ad6bf7558622d4b7 sha256值: 689a06d091ebdc4fd56e80161fed8d1febda253b684bc94016be43d3a0e37d28 sha512值: db04b4d2a94ded3c5df36ab4e45f803f859fd24dd4052d13b3a5d5fa8b6580ce6093ae051cb17a6c1c63459d3f0b0ee7ea39747cc1ad892333b1be61373f70d8 公钥算法: rsa 密钥长度: 2048 指纹: 921e9aa3c054576dfe352a96311f70f83871aa901731a7b97758639b7fcb4bb2**

## **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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| 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\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.permission.POST\_NOTIFICATIONS | 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.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.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **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。**