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

**VolkVlog（ 1.1.0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 | VolkVlog |
| 版本 | 1.1.0 |
| 包名 | com.tktk.tiktik |
| 域名线索 | 52条 |
| URL线索 | 17条 |
| APP图标 |  |
| 分析日期 | 2025年10月14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 | VolkVlog1\_0\_0\_re.apk |
| 文件大小 | 106.48MB |
| MD5值 | 48b46222e1017615b5f68a22f47cc4a9 |
| SHA1值 | 7df9b1e9b4b992ad39d9ea8f488ee0c670a35c10 |
| SHA256值 | 5c53ac68b1fa9147ee18402bfab7a18288ce53e19d2ff3994c17a01b68f741ee |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | VolkVlog |
| 包名 | com.tktk.tiktik |
| 主活动Activity | com.tktk.tiktik.MainActivity |
| 安卓版本名称 | 1.1.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| video.hollywoodstu.com | IP: 137.220.225.114  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| flvmock.tencent.com | 没有服务器地理信息. |
| api.flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| www.example.com | IP: 93.184.216.34  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| aomediacodec.github.io | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| intl-sdklog.trtc.tencent-cloud.com | IP: 43.156.86.141  所属国家: China  地区: Beijing  城市: Beijing |
| common-proxy-test.rtc.tencent.com | IP: 175.27.204.228  所属国家: China  地区: Beijing  城市: Beijing |
| livepullipv6.tlivesource.com | IP: 119.147.190.45  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 106.55.123.30 | IP: 106.55.123.30  所属国家: China  地区: Beijing  城市: Beijing |
| grs.dbankcloud.com | IP: 49.4.41.160  所属国家: China  地区: Beijing  城市: Beijing |
| common-proxy.rtc.tencent.com | IP: 106.53.137.225  所属国家: China  地区: Beijing  城市: Beijing |
| journeyapps.com | IP: 13.225.165.28  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| github.com | IP: 20.205.243.166  所属国家: United States of America  地区: Washington  城市: Redmond |
| test.tim.qq.com | IP: 106.55.123.101  所属国家: China  地区: Beijing  城市: Beijing |
| livepull.tlivesource.com | IP: 101.226.153.18  所属国家: China  地区: Shanghai  城市: Shanghai |
| tcdnsipv6.tlivesource.com | 没有服务器地理信息. |
| tcdns.tlivesource.com | IP: 109.244.168.67  所属国家: China  地区: Beijing  城市: Beijing |
| www.ietf.org | IP: 104.16.44.99  所属国家: United States of America  地区: Texas  城市: Dallas |
| 1255566655.vod2.myqcloud.com | IP: 121.51.64.177  所属国家: China  地区: Guangdong  城市: Shenzhen |
| grs.dbankcloud.eu | 没有服务器地理信息. |
| picsum.photos | IP: 104.26.5.30  所属国家: United States of America  地区: California  城市: San Francisco |
| faceidcardb.shumaidata.com | IP: 47.99.193.242  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| common-proxyintl.rtc.tencent.com | IP: 43.156.223.209  所属国家: China  地区: Beijing  城市: Beijing |
| ss8wn66.cn | IP: 116.114.96.41  所属国家: China  地区: Nei Mongol  城市: Alxa |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| inland-sdklog.trtc.tencent-cloud.com | IP: 109.244.129.219  所属国家: China  地区: Beijing  城市: Beijing |
| flutter.dev | IP: 199.36.158.100  所属国家: United States of America  地区: California  城市: Mountain View |
| vodreport.qcloud.com | IP: 150.138.36.16  所属国家: China  地区: Shandong  城市: Jinan |
| sdk-liteav-1252463788.cos.ap-hongkong.tencentcos.cn | IP: 43.128.240.61  所属国家: China  地区: Beijing  城市: Beijing |
| events.my-imcloud.com | IP: 120.53.69.253  所属国家: China  地区: Beijing  城市: Beijing |
| trtc-sdk-config-xjp-1258344699.cos.ap-singapore.intltencentcos.com | IP: 150.109.0.195  所属国家: Singapore  地区: Singapore  城市: Singapore |
| speedtest.trtc.tencent-cloud.com | IP: 162.14.6.106  所属国家: China  地区: Beijing  城市: Beijing |
| trtc-client-log-overseas-1258344699.cos.ap-singapore.intltencentcos.com | IP: 119.28.121.12  所属国家: Singapore  地区: Singapore  城市: Singapore |
| cloud.tencent.com | IP: 36.99.200.135  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mlvbdc.live.tlivesource.com | IP: 183.47.103.246  所属国家: China  地区: Guangdong  城市: Huizhou |
| developer.android.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| www.googleapis.com | IP: 172.217.160.106  所属国家: United States of America  地区: California  城市: Mountain View |
| trtc-sdk-log-1258344699.cos.ap-guangzhou.tencentcos.cn | IP: 159.75.57.195  所属国家: China  地区: Beijing  城市: Beijing |
| sdkconfig.tlivesource.com | IP: 106.55.123.30  所属国家: China  地区: Beijing  城市: Beijing |
| speedtestint.trtc.tencent-cloud.com | IP: 43.156.222.141  所属国家: China  地区: Beijing  城市: Beijing |
| avmonitortest.trtc.tencent-cloud.com | IP: 106.53.137.253  所属国家: China  地区: Beijing  城市: Beijing |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Lowestoft |
| www.volkvlog.com | IP: 137.220.225.96  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| playvideo.qcloud.com | IP: 42.81.120.58  所属国家: China  地区: Tianjin  城市: Tianjin |
| license.vod2.myqcloud.com | IP: 221.204.43.71  所属国家: China  地区: Shanxi  城市: Taiyuan |
| sdkdc.live.tlivesource.com | IP: 43.130.30.182  所属国家: China  地区: Beijing  城市: Beijing |
| life.shumaidata.com | IP: 47.111.79.97  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apisgp.my-imcloud.com | IP: 82.157.86.123  所属国家: China  地区: Beijing  城市: Beijing |
| www.webrtc.org | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| grs.dbankcloud.asia | 没有服务器地理信息. |
| grs.dbankcloud.cn | IP: 121.36.119.243  所属国家: China  地区: Guangdong  城市: Guangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview | io/flutter/plugin/platform/PlatformPlugin.java |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java |
| http://www.example.com | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java |
| https://)([\\s\\S]+) | com/huawei/hms/scankit/p/C0062bd.java |
| https://www.googleapis.com/certificateprovisioning/v1/devicecertificates/create?key=AIzaSyB-5OLKTx2iU5mko18DfdwK5611JIjbUhE | com/tencent/rtmp/TXPlayerDrmBuilder.java |
| https://cloud.tencent.com/act/event/License | com/tencent/liteav/a.java |
| https://vodreport.qcloud.com/describeControlInfos/v1/ | com/tencent/liteav/txcvodplayer/a/b.java |
| https://playvideo.qcloud.com/getplayinfo/v4 | com/tencent/liteav/txcvodplayer/b/c.java |
| http://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| https://playvideo.qcloud.com/getplayinfo/v2 | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/coverBySnapshot/1513156403\_1311093072.100\_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271\_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058\_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/master\_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d\ | com/tencent/liteav/txcvodplayer/b/d.java |
| https://journeyapps.com/ | Mogua Engine V1 |
| https://github.com/journeyapps/zxing-android-embedded | Mogua Engine V1 |
| 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://www.w3.org/Style/CSS/Test/Fonts/Ahem/). | lib/x86\_64/libflutter.so |
| https://github.com/flutter/flutter/issues. | 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://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://www.volkvlog.com | lib/armeabi-v7a/libapp.so |
| https://faceidcardb.shumaidata.com | lib/armeabi-v7a/libapp.so |
| https://picsum.photos/130/130?random= | lib/armeabi-v7a/libapp.so |
| https://life.shumaidata.com | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html | lib/armeabi-v7a/libapp.so |
| https://flutter.dev/docs/testing/errors | lib/armeabi-v7a/libapp.so |
| https://license.vod2.myqcloud.com/license/v2/1317879817\_1/v\_cube.license | lib/armeabi-v7a/libapp.so |
| https://ss8wn66.cn/tg/image\_2023-05-10\_19-02-34.png | lib/armeabi-v7a/libapp.so |
| https://picsum.photos/106/150?random= | lib/armeabi-v7a/libapp.so |
| https://t.me/VolkVlogCom | lib/armeabi-v7a/libapp.so |
| https://api.flutter.dev/flutter/material/Scaffold/of.html | lib/armeabi-v7a/libapp.so |
| https://video.hollywoodstu.com/ | 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://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip><track\_clip><clip\_id>15</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593478281.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2000</clip\_endTimeMs><clip\_playTimeMs>2000</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip></video\_track></video\_tracks><audio\_tracks><audio\_track><track\_id>1</track\_id><track\_clip><clip\_id>18</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593473438.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2206</clip\_endTimeMs><clip\_playTimeMs>2206</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip><track\_clip><clip\_id>19</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593478281.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>1950</clip\_endTimeMs><clip\_playTimeMs>1950</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip></audio\_track><audio\_track><track\_id>2</track\_id><track\_clip><clip\_id>20</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/Android/data/com.tencent.qqlive/files/mediaDownload/s0026hgpb92.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>4200</clip\_endTimeMs><clip\_playTimeMs>4200</clip\_playTimeMs><clip\_loop>0</clip\_loop><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip></audio\_track></audio\_tracks><av\_tracks><av\_track><track\_id>1</track\_id><track\_clip><clip\_id>18</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593473438.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2206</clip\_endTimeMs><clip\_playTimeMs>2206</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmCommonKey><![CDATA[drmCommonKey]]></clip\_drmCommonKey><clip\_drmOfflineKeySetId><![CDATA[drmOfflineKeySetId]]></clip\_drmOfflineKeySetId></track\_clip></av\_track></av\_tracks></assets> | lib/armeabi-v7a/libtpcore-master.so |
| http://127.0.0.1:%d/proxy/%d/%d/vod\_%d.m3u8?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/%s?play\_id=%d&clip\_id=%d&force\_online=0%s | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/master.m3u8?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/vod.mp4?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/%s.mpd\_tp\_dl\_autotype?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/%s\_tp\_dl\_autotype?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/%s?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/vod.m3u8?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/live.m3u8?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/1/%s.flv?play\_id=%d&clip\_id=1&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| http://127.0.0.1:%d/proxy/%d/%d/loop.m3u8?play\_id=%d&clip\_id=%d&force\_online=0 | lib/armeabi-v7a/libdownloadproxy.so |
| https://sdkdc.live.tlivesource.com/liteav | lib/armeabi-v7a/libliteavsdk.so |
| https://mlvbdc.live.tlivesource.com/liteav | lib/armeabi-v7a/libliteavsdk.so |
| https://intl-sdklog.trtc.tencent-cloud.com/log/report | lib/armeabi-v7a/libliteavsdk.so |
| https://inland-sdklog.trtc.tencent-cloud.com/log/report | lib/armeabi-v7a/libliteavsdk.so |
| https://106.55.123.30/rainbowapi.configs/getdatas | lib/armeabi-v7a/libliteavsdk.so |
| https://trtc-sdk-config-xjp-1258344699.cos.ap-singapore.intltencentcos.com/liteavsvrcfg/v3/serverconfig\_enc.zip | lib/armeabi-v7a/libliteavsdk.so |
| https://sdk-liteav-1252463788.cos.ap-hongkong.tencentcos.cn/sdkres/config/v2/serverconfig\_enc.zip | lib/armeabi-v7a/libliteavsdk.so |
| https://intl-sdklog.trtc.tencent-cloud.com/log/appsign | lib/armeabi-v7a/libliteavsdk.so |
| https://inland-sdklog.trtc.tencent-cloud.com/log/appsign | lib/armeabi-v7a/libliteavsdk.so |
| https://trtc-sdk-log-1258344699.cos.ap-guangzhou.tencentcos.cn | lib/armeabi-v7a/libliteavsdk.so |
| https://common-proxy.rtc.tencent.com | lib/armeabi-v7a/libliteavsdk.so |
| https://common-proxy-test.rtc.tencent.com | lib/armeabi-v7a/libliteavsdk.so |
| https://common-proxyintl.rtc.tencent.com | lib/armeabi-v7a/libliteavsdk.so |
| https://trtc-client-log-overseas-1258344699.cos.ap-singapore.intltencentcos.com | lib/armeabi-v7a/libliteavsdk.so |
| https://test.tim.qq.com | lib/armeabi-v7a/libliteavsdk.so |
| https://events.my-imcloud.com | lib/armeabi-v7a/libliteavsdk.so |
| https://apisgp.my-imcloud.com | lib/armeabi-v7a/libliteavsdk.so |
| https://speedtest.trtc.tencent-cloud.com | lib/armeabi-v7a/libliteavsdk.so |
| https://speedtestint.trtc.tencent-cloud.com | lib/armeabi-v7a/libliteavsdk.so |
| https://avmonitortest.trtc.tencent-cloud.com:8000 | lib/armeabi-v7a/libliteavsdk.so |
| http://flvmock.tencent.com | lib/armeabi-v7a/libliteavsdk.so |
| https://cloud.tencent.com/act/event/License | lib/armeabi-v7a/libliteavsdk.so |
| https://sdkconfig.tlivesource.com/rainbowapi.configs/getdatas | lib/armeabi-v7a/libliteavsdk.so |
| https://tcdns.tlivesource.com/queryip | lib/armeabi-v7a/libliteavsdk.so |
| https://tcdnsipv6.tlivesource.com/queryip | lib/armeabi-v7a/libliteavsdk.so |
| https://livepull.tlivesource.com/getpulladdr | lib/armeabi-v7a/libliteavsdk.so |
| https://livepullipv6.tlivesource.com/getpulladdr | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/armeabi-v7a/libliteavsdk.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-01 | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-02 | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-03 | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/decoding-timestamp | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-composition-time | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-type | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/armeabi-v7a/libliteavsdk.so |
| https://aomediacodec.github.io/av1-rtp-spec/ | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/armeabi-v7a/libliteavsdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/armeabi-v7a/libliteavsdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xxx@email.elided | com/tencent/liteav/base/PiiElider.java |
| camera@3x.png  home@3x.png  message@3x.png  profile@3x.png  3@3x.png  607@3x.png  427320658@3x.png  color@3x.png  flash@3x.png  switch\_camera@3x.png  square@3x.png  search@3x-2.png  search@3x.png  send@3x.png  share@3x.png  314@3x.png  矢量智能对象@3x.png  1@3x.png  33@3x.png  22@3x.png  2@3x.png  4@3x.png  427322005@3x.png  24@3x.png  heart@3x.png  group@3x.png  chat@3x.png  427321599@3x.png  triangle@3x.png  facebook@3x.png  google@3x.png  lock@3x.png  twitter@3x.png  logo@3x.png  edit@3x.png  done@3x.png  57@3x.png  58@3x.png  60@3x.png  61@3x.png  62@3x.png  63@3x.png  64@3x.png  65@3x.png  orms\_form\_list\_21786@3x.png  down@3x.png  iphone@3x.png  shop@3x.png  广告@3x.png  44@3x.png  45@3x.png  111@3x.png  fd573d24c62995dd9a2b@3x.png  75c50771ca3b77ff3023@3x.png  4d0818a44d854cb9fdbe@3x.png  6e1351a81fcb3d96d104@3x.png  36355a69ffed0ac35833@3x.png  w1@3x.png  chevron\_right@3x.png  letter@3x.png  商学院图标@3x.png  我的团队@3x.png  我的收益@3x.png  我的资产@3x.png  营收展示@3x.png  语言图标@3x.png  3757210d5c12b1fc7373@3x.png  5656a085b0777e894d8b@3x.png  nft视频@3x.png  62b8048106ae995c568d@3x.png  团队@3x.png  maticlogo@3x.png  vclogo@3x.png  vdlogo@3x.png  user@3x.png  bag@3x.png  拷贝@3x.png  37@3x.png  qr\_code@3x.png  category@3x.png  10@3x.png  13@3x.png  15.31.53@3x.png  15.31.59@3x.png  15.33.18@3x.png  15.33.22@3x.png | Mogua Engine V2 |
| ffmpeg-devel@ffmpeg.org | lib/x86/libijkplayer.so |
| ffmpeg-devel@ffmpeg.org | lib/x86\_64/libijkplayer.so |
| \_routedata@1001504625.ofroute  \_httpparser@13463476.responsepa  profile@3x.png  switch\_camera@3x.png  2@3x.png  triangle@3x.png  \_double@0150898.fromintege  \_future@4048458.immediate  \_growablelist@0150898.\_literal  heart@3x.png  \_link@14069316.fromrawpat  \_growablelist@0150898.withcapaci  \_growablelist@0150898.\_literal6  \_receiveportimpl@1026248.fromrawrec  24@3x.png  \_colorfilter@15065589.mode  \_list@0150898.\_ofarray  \_timer@1026248.periodic  \_growablelist@0150898.\_literal2  w1@3x.png  \_bigintimpl@0150898.from  \_list@0150898.empty  storationinformation@758124995.fromserial  111@3x.png  62b8048106ae995c568d@3x.png  \_directory@14069316.fromrawpat  chat@3x.png  \_casterror@0150898.\_create  \_invocationmirror@0150898.\_withtype  business@nusantara.com  down@3x.png  \_rawsocket@14069316.\_writepipe  google@3x.png  twitter@3x.png  bag@3x.png  qr\_code@3x.png  search@3x.png  \_colorfilter@15065589.lineartosr  maticlogo@3x.png  \_compressednode@362137193.single  \_hashcollisionnode@362137193.fromcollis  iphone@3x.png  \_growablelist@0150898.\_literal1  \_uri@0150898.file  square@3x.png  \_growablelist@0150898.\_literal4  \_growablelist@0150898.\_ofgrowabl  \_growablelist@0150898.of  vdlogo@3x.png  message@3x.png  lock@3x.png  \_nativesocket@14069316.pipe  camera@3x.png  \_cookie@13463476.fromsetcoo  authenticationscheme@13463476.fromstring  \_list@0150898.of  color@3x.png  \_list@0150898.generate  \_typeerror@0150898.\_create  \_list@0150898.\_ofgrowabl  shop@3x.png  \_list@0150898.\_ofefficie  \_growablelist@0150898.\_ofarray  \_growablelist@0150898.\_literal3  \_growablelist@0150898.\_ofother  5656a085b0777e894d8b@3x.png  \_timer@1026248.\_internal  \_growablelist@0150898.\_literal5  \_rawsocket@14069316.\_readpipe  \_socket@14069316.\_readpipe  category@3x.png  vclogo@3x.png  \_list@0150898.\_ofother  \_bytebuffer@7027147.\_new  ngstreamsubscription@4048458.zoned  \_assertionerror@0150898.\_create  \_nativesocket@14069316.normal  3757210d5c12b1fc7373@3x.png  \_filestream@14069316.forstdin  \_colorfilter@15065589.srgbtoline  \_host@1364032168.fromjson  \_uri@0150898.directory  \_growablelist@0150898.\_literal8  \_file@14069316.fromrawpat  1@3x.png  \_growablelist@0150898.generate  \_uri@0150898.notsimple  \_growablelist@0150898.\_literal7  \_future@4048458.zonevalue  427321599@3x.png  \_growablelist@0150898.\_ofefficie  \_future@4048458.immediatee  flash@3x.png | lib/armeabi-v7a/libapp.so |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libijkplayer.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.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: CN=1, OU=1, O=1, L=1, ST=1, C=US 签名算法: rsassa\_pkcs1v15 有效期自: 2023-05-22 02:41:29+00:00 有效期至: 2048-05-15 02:41:29+00:00 发行人: CN=1, OU=1, O=1, L=1, ST=1, C=US 序列号: 0x1 哈希算法: sha256 md5值: 8b68091d22b8c46e6d8c1ac6e8c76a9e sha1值: 39ec160ee5dfe53fcf8923ae1659f777d0ce2bab sha256值: b9fd7afe49e791c77e2c727d4856d30c90473b9b76156dc0ea54ecce4fd2e4dc sha512值: 068d6d26195dd2db592aab475130a424b2e71bf31ec13f99c4541bd37ec5062cd30a8c63d7041617793d5edb58d9aed0844b2fc9e766092ad3a3f1d9903d3185 公钥算法: rsa 密钥长度: 2048 指纹: 4f99777bafeb751d52de42c065fe8847b3ff06d7c8f0401aed403e0da08ce4c7**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "library\_zxingandroidembedded\_author" : "JourneyApps" |
| "library\_zxingandroidembedded\_authorWebsite" : "https://journeyapps.com/" |

## **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.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.READ\_PHONE\_NUMBERS | 危险 |  | 允许到设备的读访问的电话号码。这是 READ\_PHONE\_STATE 授予的功能的一个子集,但对即时应用程序公开 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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 |
| 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.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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.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 |
| com.tktk.tiktik.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tktk.tiktik.MainActivity | **Schemes**: tiktik://, |

**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。**