



MoGua

东京 8.0.8.APK 分析报告



APP名称:	东京
包名:	com.la4eb7eba6.mdnr
域名线索:	29条
URL线索:	28条
邮箱线索:	4条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

📁 文件信息

文件名: 东京.apk
文件大小: 77.18MB
MD5值: 81bc0f368df975670a2bba5a36aa87fc
SHA1值: 23264528861bf6cce1d12cb867f10d36c62d6a83
SHA256值: 25f8161e5063e94c0f4426dedf510cd28c5bf9460f6db2e74a7d91a8ce408fdd

i APP 信息

App名称: 东京
包名: com.la4eb7eba6.mdnr
主活动Activity: com.la4eb7eba6.mdnr.MainActivity
安卓版本名称: 8.0.8
安卓版本: 1

🔍 域名线索

域名	服务器信息
dartbug.com	IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
developer.android.com	IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
aomediacodec.github.io	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.example.com	IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
stackoverflow.com	IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
ac.dun.163.com	IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
1255566655.vod2.myqcloud.com	IP: 124.163.195.59 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
ns.adobe.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 纬度: 37.405991 经度: -122.078514

ac.dun.163yun.com	IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
da.dun.163.com	IP: 59.111.211.178 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
playvideo.qcloud.com	IP: 119.188.180.230 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
crash.163.com	IP: 45.254.50.146 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
paulbakaus.com	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
www.ietf.org	IP: 104.16.45.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cloud.tencent.com	IP: 60.28.220.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
www.webrtc.org	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.ibm.com	IP: 2.19.154.251 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London 纬度: 51.508530 经度: -0.125740
dev.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
docs.flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
flutter.dev	IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.unicode.org	IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204
schemas.android.com	没有服务器地理信息.
10.0.2.2	IP: 10.0.2.2 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

URL线索

URL信息	Uri所在文件
http://schemas.android.com/apk/res/android	com/humrousz/sequence/AnimationImageView.java
https://ac.dun.163yun.com	com/netease/mobsec/c/a.java
https://ac.dun.163.com	com/netease/mobsec/c/a.java
https://ac.dun.163.com/v2/config/android?	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/config/android?	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/m/d	com/netease/mobsec/f/f.java
https://ac.dun.163.com/v2/m/d	com/netease/mobsec/f/f.java
https://ac.dun.163yun.com/v2/m/b	com/netease/mobsec/f/f.java
https://ac.dun.163.com/v2/m/b	com/netease/mobsec/f/f.java
https://crash.163.com/uploadCrashLogInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://crash.163.com/client/api/uploadStartUpInfo.do	com/netease/nis/basesdk/crash/BaseJavaCrashHandler.java
https://da.dun.163.com/sn.gif?d=	com/netease/nis/captcha/g.java
http://www.example.com	com/pichillilorenzo/flutter_inappwebview_android/chrome_custom_tabs/CustomTabsHelper.java
https://cloud.tencent.com/act/event/License	com/tencent/iteav/a.java
http://playvideo.qcloud.com/getplayinfo/v2	com/tencent/iteav/txcvodplayer/b/d.java
https://playvideo.qcloud.com/getplayinfo/v2	com/tencent/iteav/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/iteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/iteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3\	com/tencent/iteav/txcvodplayer/b/d.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4\	com/tencent/iteav/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://docs.flutter.dev/deployment/android	io/flutter/embedding/engine/loader/FlutterLoader.java
https://developer.android.com/guide/topics/permissions/overview	io/flutter/plugin/platform/PlatformPlugin.java
http://10.0.2.2:8969/stream	io/sentry/SpotlightIntegration.java
https://github.com/Baseflow/flutter-permission-handler/issues	l/p.java
https://github.com/yyued/SVGAPlayer-Android	t5/g.java
https://github.com/nodeca/pica	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
https://www.gnu.org/licenses/>.	摸瓜V2引擎
http://paulbikaus.com/tutorials/html5/web-audio-on-ios/	摸瓜V2引擎
http://stackoverflow.com/questions/24119684	摸瓜V2引擎
https://github.com/richttr/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
http://ns.adobe.com/xap/1.0/	lib/armeabi/libimagepipeline.so
http://www.webrtc.org/experiments/rtp-hdext/generic-frame-descriptor	lib/armeabi-v7a/libagora-rtc-sdk.so
http://s	lib/armeabi-v7a/libagora-rtc-sdk.so
http://127.0.0.1:	lib/armeabi-v7a/libapp.so

http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd	lib/armeabi-v7a/libapp.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/armeabi-v7a/libapp.so
http://127.0.0.1:88888/	lib/armeabi-v7a/libapp.so
http://kiwi_live/tunnel/a033b072?z=1&nobase64=1	lib/armeabi-v7a/libapp.so
https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.	lib/armeabi-v7a/libapp.so
http://kiwi_install	lib/armeabi-v7a/libapp.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
http://www.unicode.org/copyright.html	lib/armeabi-v7a/libflutter.so
https://docs.flutter.dev/release/breaking-changes/android-surface-plugins	lib/armeabi-v7a/libflutter.so
https://github.com/flutter/flutter/issues.	lib/armeabi-v7a/libflutter.so
https://dartbug.com/52121.	lib/armeabi-v7a/libflutter.so
http://www.webrtc.org/experiments/rtp-hdext/abs-send-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdext/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-hdext/meta-data-01	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdext/meta-data-02	lib/armeabi-v7a/libliteavsdk.so

http://www.webrtc.org/experiments/rtp-hdrex/meta-data-03	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/decoding-timestamp	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/video-composition-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/video-frame-type	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/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-hdrex/generic-frame-descriptor-00	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/abs-capture-time	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/video-content-type	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/video-timing	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/color-space	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/inband-cn	lib/armeabi-v7a/libliteavsdk.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so
http://www.webrtc.org/experiments/rtp-hdrex/generic-frame-descriptor	lib/arm64-v8a/libagora-rtc-sdk.so
http://s	lib/arm64-v8a/libagora-rtc-sdk.so
https://api.flutter.dev/flutter/material/Scaffold/of.html	lib/arm64-v8a/libapp.so

 邮箱线索

邮箱地址	所在文件
xxx@email.elided	com/tencent/liteav/base/PiiElider.java
u0013android@android.com0 u0013android@android.com	w2/q.java
_growablelist@0150898._literal _typeerror@0150898._create _xfa@56287047.wqd _bytebuffer@7027147._new _double@0150898.fromintege _immutablelist@0150898._tk _assertionerror@0150898._create	lib/armeabi-v7a/libapp.so
appro@openssl.org	lib/arm64-v8a/libagora-rtc-sdk.so

手机线索

手机号	所在文件
17512775099	i4/a.java

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=63, ST=horizontal, L=horizontal, O=horizontal, OU=horizontal, CN=horizontal
签名算法: dsa
有效期自: 2024-12-05 07:04:23+00:00
有效期至: 2025-12-05 07:04:23+00:00
发行人: C=63, ST=horizontal, L=horizontal, O=horizontal, OU=horizontal, CN=horizontal
序列号: 0x6b269d8b
哈希算法: sha256
md5值: f1deea8dc8f82e192d1e0a836aa38c6e
sha1值: 4f685896c426946bc20a3032c685a8004372c30e
sha256值: d5577d7edc8657475932abf2f87a68ff6f697b82d625062e42047a5713895c5b
sha512值: 27492ea96f555850c0688a64660c77b61b06a52ac30ea48197ae0a3247d89d8d85c36c7e1cc2c4f47745b1b4a7c9c02ce524d9ad1a2b55670e88029429aa1f60
公钥算法: dsa
密钥长度: 2048
指纹: be276df14fc0ab11f005b5fd9778f9d8faadd46782c081f9d3c70e4281368578

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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_MEDIA_VISUAL_USER_SELECTED	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.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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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_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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.POST_NOTIFICATIONS	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。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
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.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
com.la4eb7eba6.mdnr.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	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_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference

应用内通信