



MoGua

玖玖医养 4.0.1130.APK 分析报告



APP名称:

玖玖医养

包名:	com.jnhc.yiyang
域名线索:	40条
URL线索:	24条
邮箱线索:	0条
分析日期:	2025年6月26日
分析平台:	摸瓜APK反编译平台

文件名: app-armeabi-v7a-release_sig.apk
文件大小: 19.7MB
MD5值: 59f9533a058ec721fe670417c6174fd7
SHA1值: bd3516fe34468fc1ba06c586b8b39fd2ed8cf869
SHA256值: c6432cddaf914d78ab49afd90f87dff47ab640099ce4437708466f1b4bacb2cc

i APP 信息

App名称: 玖玖医养
包名: com.jnhc.yiyang
主活动Activity: com.jnhc.yiyang.activity.HomeActivity
安卓版本名称: 4.0.1130
安卓版本: 55

🔍 域名线索

域名	服务器信息
tools.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
r.avlab.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
common-proxy.rtc.tencent.com	IP: 106.55.209.148 所属国家: China 地区: Beijing

	城市: Beijing 纬度: 39.907501 经度: 116.397102
common-proxyintl rtc.tencent.com	IP: 43.156.255.121 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
cloud-test.tim.qq.com	IP: 106.55.120.32 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ping.huatuo.qq.com	IP: 220.194.111.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.videolan.org	IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.859077 经度: 2.293486
jiujiu.jiujiuhealthcare.com	IP: 10.255.218.72 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

common-proxy-test.rtc.tencent.com	IP: 175.27.204.228 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
speedtestint.trtc.tencent-cloud.com	IP: 43.156.86.158 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
access.sdgcms.com	没有服务器地理信息.
tcdns.myqcloud.com	IP: 109.244.168.67 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
livepull.myqcloud.com	IP: 116.130.223.85 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
119.29.29.98	IP: 119.29.29.98 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
	IP: 43.130.137.30 所属国家: United States of America 地区: Virginia

sdkdc.live.qcloud.com	城市: Ashburn 纬度: 39.039474 经度: -77.491806
example.com	IP: 23.192.228.84 所属国家: United States of America 地区: California 城市: Santa Clara 纬度: 37.354111 经度: -121.955490
test.tim.qq.com	IP: 106.55.123.101 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
restapi.amap.com	IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
livepullipv6.myqcloud.com	IP: 163.177.30.38 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.ietf.org	IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

speedtest.trtc.tencent-cloud.com	IP: 162.14.20.26 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
lanvideo.jiujiuhealthcare.com	IP: 10.255.218.228 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
trtc-sdk-log-1258344699.cos.ap-guangzhou.myqcloud.com	IP: 36.248.13.176 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390 经度: 119.306107
dldir1v6.qq.com	IP: 119.188.86.132 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
avmonitortest.trtc.tencent-cloud.com	IP: 106.53.137.253 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
inland-sdklog.trtc.tencent-cloud.com	IP: 120.53.101.57 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
ipv6-datacenter.live.qcloud.com	IP: 183.47.109.107 所属国家: China 地区: Guangdong 城市: Huizhou 纬度: 39.509766 经度: 116.693001
reddit-1258344699.cos.na-siliconvalley.myqcloud.com	IP: 170.106.97.195 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418
intl-sdklog.trtc.tencent-cloud.com	IP: 43.153.191.214 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
trtc-sdk-config-1258344699.file.myqcloud.com	IP: 221.204.14.81 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
tcdnsipv6.myqcloud.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
	IP: 116.196.151.115 所属国家: China

liteav.sdk.qcloud.com	地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
10.255.218.71	IP: 10.255.218.71 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
yun.tim.qq.com	IP: 60.29.232.78 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
www.webrtc.org	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
cloud.tim.qq.com	IP: 111.206.149.220 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

162.14.6.247	IP: 162.14.6.247 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
hwapi.im.qcloud.com	没有服务器地理信息.

 URL线索

URL信息	Url所在文件
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/carousel/img/getCarousel	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/resources/video/list/list	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/jjyy/camera/bindCamera	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/jjyy/socket/bindSocket	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/jjyy/users/getUserNameByWs	com/jnhc/yiyang/util/net/URL.java

http://10.255.218.71:8081/gateway/sm-admin/front/counsole/save	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sys/dict/getDictByTN	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sys/dict/getDictsByType	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/healthData/getSelectData	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/column/getDataByPid	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/bussiness/getBussiness	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8082/resources/	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/jjyy/camera/ifBind	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sys/resources/video/list/list	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sys/resources/video/getPlayUrl	com/jnhc/yiyang/util/net/URL.java
http://10.255.218.71:8081/gateway/sm-admin/back/tencentPush/send	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/jjyy/sms/sendDoctorNotice	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sm/app_two/sys-package/checkNumber	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v1/sm/sys/ws-loginout-record/add	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sm/app_two/sys-	

package/deduct	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/resources/video/indexOne	com/jnhc/yiyang/util/net/URL.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/resources/video/record/add	com/jnhc/yiyang/util/net/URL.java
https://restapi.amap.com/v3/weather/weatherInfo?key=660cfe15f76aaca32977016d60e928f0&extensions=all&city=	com/jnhc/yiyang/util/net/URL.java
https://lanvideo.jiujiuhealthcare.com:9000/vcs/account/login	com/jnhc/yiyang/util/net/VideoRequest.java
https://lanvideo.jiujiuhealthcare.com:9000/vcs/room/members	com/jnhc/yiyang/util/net/VideoRequest.java
https://lanvideo.jiujiuhealthcare.com:9000/vcs/room/enter	com/jnhc/yiyang/util/net/VideoRequest.java
http://jiujiu.jiujiuhealthcare.com:8083/	com/jnhc/yiyang/activity/XiangqingActivity.java
http://jiujiu.jiujiuhealthcare.com:8083?version=25&token=	com/jnhc/yiyang/activity/YiyangPreviewActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-auth/login	com/jnhc/yiyang/activity/GuideActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/carousel/img/getCarousel?type=6	com/jnhc/yiyang/activity/GuideActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-auth/login	com/jnhc/yiyang/activity/HomeActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/carousel/img/getCarousel?type=6	com/jnhc/yiyang/activity/HomeActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-auth/login	com/jnhc/yiyang/activity/AdvertActivity.java
http://access.sdgdcms.com/account/user/get_list?devicetype=1&deviceno=	com/jnhc/yiyang/activity/AdvertActivity.java

http://access.sdgdcms.com/account/login?deviceno=	com/jnhc/yiyang/activity/AdvertActivity.java
http://jiujiu.jiujiuhealthcare.com:8083/	com/jnhc/yiyang/activity/media/CommodityActivity.java
http://jiujiu.jiujiuhealthcare.com:8083/	com/jnhc/yiyang/activity/media/MediaActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sys/resources/video/list/list?id=	com/jnhc/yiyang/activity/media/MediaActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-adminsm/api/v2/sys/resources/video/getPlayUrl?videoid=	com/jnhc/yiyang/activity/media/MediaActivity.java
http://jiujiu.jiujiuhealthcare.com:8083/	com/jnhc/yiyang/activity/media/BigDoctorActivity.java
http://jiujiu.jiujiuhealthcare.com:8081/gateway/sc-admin/api/v1/sys/resources/video/list/list?id=	com/jnhc/yiyang/activity/media/BigDoctorActivity.java
http://jiujiu.jiujiuhealthcare.com:8083/gateway/sc-adminsm/api/v1/sm/jjyy/users/getUserNameByWs?wsid=	com/jnhc/yiyang/activity/call/VideoCallActivity.java
https://lanvideo.jiujiuhealthcare.com:9000/vcs/	com/jnhc/yiyang/base/BaseApplication.java
https://lanvideo.jiujiuhealthcare.com:9000/vcs/	com/jnhc/yiyang/base/ECAApplication.java
http://%s/timeshift/%s/%s/timeshift.m3u8?delay=%d	com/tencent/liteav/j.java
http://%s/%s/%s/timeshift.m3u8?starttime=%s&appid=%s&txKbps=0	com/tencent/liteav/j.java
http://%s/timeshift/%s/%s/timeshift.m3u8?delay=0	com/tencent/liteav/j.java
http://%s/%s/%s/timeshift.m3u8?delay=0&appid=%s&txKbps=0	com/tencent/liteav/j.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar1.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar2.png	com/tencent/liteav/basic/AvatarConstant.java

https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar3.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar4.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar5.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar6.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar7.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar8.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar9.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar10.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar11.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar12.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar13.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar14.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar15.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar16.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar17.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar18.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar19.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar20.png	com/tencent/liteav/basic/AvatarConstant.java

https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar21.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar22.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar23.png	com/tencent/liteav/basic/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar24.png	com/tencent/liteav/basic/AvatarConstant.java
https://livepull.myqcloud.com/getpulladdr	com/tencent/liteav/network/h.java
https://livepullipv6.myqcloud.com/getpulladdr	com/tencent/liteav/network/h.java
https://tcdns.myqcloud.com/queryip	com/tencent/liteav/network/c.java
https://tcdnsipv6.myqcloud.com/queryip	com/tencent/liteav/network/c.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar1.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar2.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar3.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar4.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar5.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar6.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar7.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar8.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar9.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java

https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar10.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar11.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar12.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar13.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar14.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar15.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar16.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar17.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar18.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar19.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar20.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar21.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar22.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar23.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
https://liteav.sdk.qcloud.com/app/res/picture/voiceroom/avatar/user_avatar24.png	com/tencent/liteav/trtccalling/model/util/AvatarConstant.java
http://example.com/	cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java
http://162.14.6.247/v4/ConfigGetSvc/GetOpenSSOIPList	lib/armeabi-v7a/liblmsdk.so
https://ping.huatuo.qq.com/api.im.qcloud.com	lib/armeabi-v7a/liblmsdk.so

http://119.29.29.98/d?id=3743	lib/armeabi-v7a/libImSDK.so
http://www.videolan.org/x264.html	lib/armeabi-v7a/libanylive.3.3.3.so
https://yun.tim.qq.com	lib/armeabi-v7a/libliteavsdk.so
https://speedtest.trtc.tencent-cloud.com	lib/armeabi-v7a/libliteavsdk.so
https://test.tim.qq.com	lib/armeabi-v7a/libliteavsdk.so
https://avmonitortest.trtc.tencent-cloud.com:8000	lib/armeabi-v7a/libliteavsdk.so
https://hwapi.im.qcloud.com	lib/armeabi-v7a/libliteavsdk.so
https://speedtestint.trtc.tencent-cloud.com	lib/armeabi-v7a/libliteavsdk.so
https://reddit-1258344699.cos.na-siliconvalley.myqcloud.com	lib/armeabi-v7a/libliteavsdk.so
https://intl-sdklog.trtc.tencent-cloud.com/log/appsign	lib/armeabi-v7a/libliteavsdk.so
https://intl-sdklog.trtc.tencent-cloud.com/log/report	lib/armeabi-v7a/libliteavsdk.so
https://trtc-sdk-log-1258344699.cos.ap-guangzhou.myqcloud.com	lib/armeabi-v7a/libliteavsdk.so
https://inland-sdklog.trtc.tencent-cloud.com/log/appsign	lib/armeabi-v7a/libliteavsdk.so
https://inland-sdklog.trtc.tencent-cloud.com/log/report	lib/armeabi-v7a/libliteavsdk.so
https://trtc-sdk-config-1258344699.file.myqcloud.com/liteavsrcfg/android/serverconfig_en.zip	lib/armeabi-v7a/libliteavsdk.so
https://dldir1v6.qq.com/hudongzhibo/liteavsrcfg/serverconfig_en.zip	lib/armeabi-v7a/libliteavsdk.so
https://sdkdc.live.qcloud.com/liteav	lib/armeabi-v7a/libliteavsdk.so

https://ipv6-datacenter.live.qcloud.com/liteav	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://common-proxy.rtc.tencent.com	lib/armeabi-v7a/libliteavsdk.so
https://liteav.sdk.qcloud.com/sdkres/trtc/AiVoiceEnhancement/Android/XNN_Android_1.0.zip	lib/armeabi-v7a/libliteavsdk.so
https://cloud.tim.qq.com/v3/liveinterface/	lib/armeabi-v7a/libliteavsdk.so
https://cloud-test.tim.qq.com/v3/liveinterface/	lib/armeabi-v7a/libliteavsdk.so
http://r.avlab.qq.com	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time	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/transport-wide-cc-02	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrext/playout-delay	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://tools.ietf.org/html/draft-ietf-avtext-framemarking-07	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/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-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/order-in-stream	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/generic-frame-descriptor-01	lib/armeabi-v7a/libliteavsdk.so
http://www.webrtc.org/experiments/rtp-hdrex/meta-data	lib/armeabi-v7a/libliteavsdk.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libtxffmpeg.so

 邮箱线索

 手机线索

手机号	所在文件
18369201693	com/jnhc/yiyang/service/VideoService.java

 签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: CN=btn
签名算法: rsassa_pkcs1v15
有效期自: 2018-03-28 07:50:24+00:00
有效期至: 2043-03-22 07:50:24+00:00
发行人: CN=btn
序列号: 0x45ca98ba
哈希算法: sha256
md5值: 83de6e4759392c967e00075f5928003e
sha1值: 9a934ace090198e7799364354ff79d22c7685437
sha256值: 242a43226fc89bb584afcd0293ffcb707890cacdf9979dc47084ed77899ee6b
sha512值: 4472d40cee10466f482ff525d779995c029a48b632c6325117ebe9d8a3868830499ccff3b5b3e9c75d29f581097ee10a3fd8ecffe6dd99b23b4c03390ec1388d

硬编码敏感信息

可能的敏感信息
"illegal_user_name" : "非法用户名"
"password" : "Password"
"user_name" : "User name"

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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_mock_location	危险	用于测试的模拟位置源	创建模拟位置源进行测试。恶意应用程序可以使用它来覆盖由真实位置源（如 GPS 或网络提供商）返回的位置和/或状态
android.permission.WRITE_EXTERNAL_STORAGE	危险	读取/修改/删除外部存储内容	允许应用程序写入外部存储
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

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.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.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.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.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.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.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.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.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.CAPTURE_VIDEO_OUTPUT	正常		允许应用程序捕获视频输出
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话

应用内通信