



MoGua

果博东方 1.0.APK 分析报告



APP名称:

果博东方

包名:

com.dyb.newgppto

域名线索:

12条

URL线索:	14条
邮箱线索:	2条
分析日期:	2024年4月25日
分析平台:	摸瓜反编译平台

文件信息

文件名: base.apk
文件大小: 9.68MB
MD5值: dc65799b0a2e64e092fbe78576d05a08
SHA1值: 84780d1641dd46d67190acbaae69a70c7ad01adb
SHA256值: 9c0dd28f3e080aad457849b197ff59bd8b36051e9ef44c8b2f50efa221abc117

APP 信息

App名称: 果博东方

包名: com.dyb.newgprto
主活动Activity: com.dyb.newgprto.SplashActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
www.openssl.org	IP: 72.247.15.217 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683
playvideo.qcloud.com	IP: 103.18.209.60 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
upload.ffmpeg.org	IP: 213.36.253.119 所属国家: France 地区: Ile-de-France 城市: Paris 纬度: 48.853409 经度: 2.348800
1255566655.vod2.myqcloud.com	IP: 182.254.53.33 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
livepull.myqcloud.com	IP: 183.47.114.223 所属国家: China 地区: Guangdong 城市: Huizhou 纬度: 23.083330 经度: 114.400002

dldir1.qq.com	IP: 182.254.59.238 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
192.168.2.103	IP: 192.168.2.103 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
tcdns.myqcloud.com	IP: 106.55.123.19 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
yun.tim.qq.com	IP: 49.233.104.16 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
g-oss.oss-accelerate.aliyuncs.com	IP: 39.107.134.53 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
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: 116.397232
	IP: 183.47.97.245 所属国家: China

mlvbdc.live.qcloud.com	地区: Guangdong 城市: Huizhou 纬度: 23.083330 经度: 114.400002
------------------------	---

 URL线索

URL信息	Url所在文件
http://%s/timeshift/%s/%s/timeshift.m3u8?delay=%d	com/tencent/liteav/d.java
http://%s/%s/%s/timeshift.m3u8?starttime=%s&appid=%s&txKbps=0	com/tencent/liteav/d.java
http://%s/timeshift/%s/%s/timeshift.m3u8?delay=0	com/tencent/liteav/d.java
http://%s/%s/%s/timeshift.m3u8?delay=0&appid=%s&txKbps=0	com/tencent/liteav/d.java
http://dldir1.qq.com/hudongzhibo/liteavsvrcfg/serverconfig_en.zip	com/tencent/liteav/basic/e/b.java
https://livepull.myqcloud.com/getpulladdr	com/tencent/liteav/network/k.java
http://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/network/f.java
https://playvideo.qcloud.com/getplayinfo/v2	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/coverBySnapshot/1513156403_1311093072.100_0.jpg?t=5c08d9fa&us=someus&sign=95f34beb353fe32cfe7f8b5e79cc28b1	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271_00001.jpg?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/imageSprite/1513156058_533711271.vtt?t=5c08d9fa&us=someus&sign=79449db4e1fb05a3becfa096613659c3	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/ca754badvodgzp1255566655/8f5fbff14564972818519602447/uAnXX0OMLSAA.wmv?t=5c08d9fa&us=someus&sign=659af5dd3f27eb92dc4ed74eb561daa4	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/master_playlist.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java

http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f220.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f230.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f240.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f210.m3u8?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f10.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
http://1255566655.vod2.myqcloud.com/7e9cee55vodtransgzp1255566655/8f5fbff14564972818519602447/v.f20.mp4?t=5c08d9fa&us=someus&sign=66290475b7182c89193f03b8f74a979d	com/tencent/liteav/network/f.java
https://tcdns.myqcloud.com/queryip	com/tencent/liteav/network/c.java
http://g-oss.oss-accelerate.aliyuncs.com/new/v	com/ccc/ossweb/H5Container.java
http://g-oss.oss-accelerate.aliyuncs.com/new/g.zip	com/ccc/ossweb/H5Container.java
http://g-oss.oss-accelerate.aliyuncs.com/new/gb_android	com/ccc/ossweb/H5Container.java
http://192.168.2.103/g.zip	com/ccc/ossweb/H5Game.java
http://192.168.2.103/v	com/ccc/ossweb/H5Game.java
ftp://upload.ffmpeg.org/incoming/	lib/armeabi-v7a/libtxplayer.so
http://mlvbdc.live.qcloud.com/	lib/armeabi-v7a/libliteavsdk.so
http://objaaaafhiehjjf/ohae.oiaa	lib/armeabi-v7a/libliteavsdk.so
https://yun.tim.qq.com	lib/armeabi-v7a/libliteavsdk.so
https://test.tim.qq.com	lib/armeabi-v7a/libliteavsdk.so

http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libtxffmpeg.so
ftp://upload.ffmpeg.org/incoming/	lib/arm64-v8a/libtxplayer.so
http://mlvbdc.live.qcloud.com/	lib/arm64-v8a/libliteavsdk.so
https://yun.tim.qq.com	lib/arm64-v8a/libliteavsdk.so
https://test.tim.qq.com	lib/arm64-v8a/libliteavsdk.so
http://objaaaafhiehjjf/ohae.oiaa	lib/arm64-v8a/libliteavsdk.so
http://www.openssl.org/support/faq.html	lib/arm64-v8a/libtxffmpeg.so

 邮箱线索

邮箱地址	所在文件
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libtxplayer.so
ffmpeg-devel@ffmpeg.org	lib/arm64-v8a/libtxplayer.so

 手机线索

手机号	所在文件
17179869184	com/tencent/ijk/media/player/IjkMediaMeta.java

 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False

Found 1 unique certificates
Subject: C=sdgdsaggd, ST=gdsg, L=dsgdsaggdsg, O=gdsg, OU=dgsgs, CN=dsgds
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-25 15:49:43+00:00
Valid To: 2044-08-18 15:49:43+00:00
Issuer: C=sdgdsaggd, ST=gdsg, L=dsgdsaggdsg, O=gdsg, OU=dgsgs, CN=dsgds
Serial Number: 0x7cacf22e
Hash Algorithm: sha256
md5: e3b8f97b525f5300974b8a1d911093bc
sha1: eb879d90ec9133baab1c91d1662ca19dba0fa214
sha256: bc5f6708d5719815b311af1878575041edfa768e337ef43b215165e899e59d00
sha512: 5c1610dacf2277cff8c3a85cb66925db7f27fe978ab1b38bf23128af9ff02870b2c31e82503a04fd1d77765819ce2c854e081ed1fdf808051501da095629d1fe
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 07393548c68167a7686c1eb7d90b3590f0d2b554dc4e7382940a061f2697aab5

硬编码敏感信息

加壳分析

第三方SDK

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.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

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。