



MoGua

主播视频 1.2.2.APK 分析报告



APP名称:

主播视频

包名:	com.zb.video3_18
域名线索:	17条
URL线索:	38条
邮箱线索:	3条
分析日期:	2025年10月14日
分析平台:	摸瓜APK反编译平台

文件名: 123.apk
文件大小: 14.18MB
MD5值: 230c337d9552b8485b545c03337cf307
SHA1值: 14db8011678bc7ae54abec73c2d4c5c654565e01
SHA256值: 977b3d65d69c983aebfc2af61cdcbea6efabfb49b6b88d3e7252cc42cfc8c547

i APP 信息

App名称: 主播视频
包名: com.zb.video3_18
主活动Activity: com.zhubo.zhubo001.mvp.ui.activity.SplashActivity
安卓版本名称: 1.2.2
安卓版本: 122

🔍 域名线索

域名	服务器信息
greenrobot.org	IP: 85.13.163.69 所属国家: Germany 地区: Thuringen 城市: Friedersdorf 纬度: 50.604919 经度: 11.035770
image.17flying.cc	没有服务器地理信息.
api.github.com	IP: 20.205.243.168 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281

api.v8dw3c.shop	没有服务器地理信息.
alj1s9j1.com	IP: 194.53.53.245 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
log.hnqfnnb.space	没有服务器地理信息.
api.babeweb.xyz	IP: 18.223.214.123 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961380 经度: -82.997749
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
help.kuaiyun.cloud	没有服务器地理信息.
ip.zxinc.org	IP: 101.32.207.56 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
aria.laoyuyu.me	IP: 118.24.25.24 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397102
pagead2.google syndication.com	IP: 58.254.149.166 所属国家: China 地区: Guangdong 城市: Yunfu 纬度: 22.930559 经度: 112.037300
wwiy.lanzouj.com	IP: 221.204.43.72 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
img.zcool.cn	IP: 42.59.6.99 所属国家: China 地区: Liaoning 城市: Dalian 纬度: 41.069592 经度: 122.598511
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
qp.java444.com	没有服务器地理信息.
www.sl4j.org	IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790

URL线索

URL信息	Url所在文件
https://aria.laoyuyu.me/aria_doc/create/any_java.html	com/arialyy/aria/core/Aria.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/download/DownloadReceiver.java
https://github.com/AriaLyy/Aria/issues/597	com/arialyy/aria/core/download/m3u8/M3U8Option.java
https://aria.laoyuyu.me/aria_doc/other/annotaion_invalid.html	com/arialyy/aria/core/upload/UploadReceiver.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/m.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://github.com/danikula/AndroidVideoCache/issues/43	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/88	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache3/hls/FileUtils.java
http://%s:%d/%s	com/danikula/videocache3/server/HttpProxyCacheServer.java
http://%s:%d/%s	com/danikula/videocache3/server/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134	com/danikula/videocache3/server/Pinger.java

https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache3/server/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache3/server/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache3/server/HttpUrlSource.java
https://api.github.com/	com/jess/arms/a/b/p.java
http://xml.apache.org/xslt	com/jess/arms/c/b.java
https://alj1s9j1.com/	com/re/ng/yhqp/Client.java
https://image.17flying.cc/uploads/20200311/038086d71050749638b80160d8185a0b.png	com/re/ng/yhqp/bean/GameBean.java
http://qp.java444.com/game/into	com/re/ng/yhqp/bean/GameBean.java
https://wwiy.lanzouj.com/b04wufgra	com/zhubo/zhubo001/c/a/b.java
https://wwiy.lanzouj.com/b04wufgra	com/zhubo/zhubo001/e/g0.java
https://ip.zxinc.org/api.php?type=json	com/zhubo/zhubo001/e/l1/a.java
https://log.hnqfnnb.space/cloud-upload/upload3/posts	com/zhubo/zhubo001/e/l1/a.java
http://api.babeweb.xyz/fast-cloud/	com/zhubo/zhubo001/mvp/model/api/Api.java
https://api.v8dw3c.shop/fast-cloud/	com/zhubo/zhubo001/mvp/model/api/Api.java
https://help.kuaiyun.cloud/	com/zhubo/zhubo001/mvp/model/api/Api.java
https://img.zcool.cn/community/011ad05e27a173a801216518a5c505.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/0148fc5e27a173a8012165184aad81.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java

https://img.zcool.cn/community/013c7d5e27a174a80121651816e521.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01b8ac5e27a173a80120a895be4d85.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01a85d5e27a174a80120a895111b2c.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01085d5e27a174a80120a8958791c4.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://img.zcool.cn/community/01f8735e27a174a8012165188aa959.jpg	com/zhubo/zhubo001/mvp/model/enity/netbean/BannerDataBean.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	d/b/a/a/a/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/a.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/i.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/f.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/w.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/n.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/c.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/l.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/g.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java

https://greenrobot.org/greendao/documentation/database-encryption/	org/greenrobot/greendao/h/b.java
http://www.slf4j.org/codes.html	org/slf4j/c.java

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	com/danikula/videocache/HttpUrlSource.java
danikula@gmail.com	com/danikula/videocache3/server/HttpUrlSource.java
nzbsp999@gmail.com	com/zhubo/zhubo001/mvp/ui/activity/SplashActivity.java

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.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=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com

签名算法: rsassa_pkcs1v15
 有效期自: 2008-02-29 01:33:46+00:00
 有效期至: 2035-07-17 01:33:46+00:00
 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
 序列号: 0x936eacbe07f201df
 哈希算法: sha1
 md5值: e89b158e4bcf988ebd09eb83f5378e87
 sha1值: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
 sha256值: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
 sha512值: 5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569
 公钥算法: rsa
 密钥长度: 2048
 指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

硬编码敏感信息

可能的敏感信息
"dialog_auth_btn" : "去认证"
"et_card_pwd_hit" : "请输入身份卡密码"
"google_api_key" : "AlzaSyBGVujDnG-P7crPpplUPAbKAjQeMGHfL2w"
"google_crash_reporting_api_key" : "AlzaSyBGVujDnG-P7crPpplUPAbKAjQeMGHfL2w"
"login_forget_pwd" : "忘记密码"
"login_mode_pwd" : "注册账号登录"
"login_toast_forget_pwd_success" : "找回密码成功。请尝试登录"
"login_toast_pwd_length" : "请输入6~20位密码"
"login_toast_pwd_wrong" : "密码错误"

"pwd_limit" : "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ"
"token_erc" : "ERC-20"
"token_trc" : "TRC-20"
"token_type_label" : "类型"

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	类型	详细情况

	险		
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
	正		

android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.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.PERMISSIONS_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.zhubo.zhubo001.mvp.ui.activity.MainActivity	Schemes: cdpk7155://,
com.zhubo.zhubo001.mvp.ui.activity.SplashActivity	Schemes: cdpk7155://,