



MoGua

U蓝视频 2.1.2.APK 分析报告



APP名称:

U蓝视频

包名:	info.lkdlyb.wvd.kptr
域名线索:	24条
URL线索:	23条
邮箱线索:	1条
分析日期:	2025年5月22日
分析平台:	摸瓜APK反编译平台

文件名: ul_2.1.2.apk
文件大小: 17.48MB
MD5值: 9a5f4d59bad3bdde13dc0f222a9d66e9
SHA1值: 6a0be7203a95bf53c7f0bf5872b76738d654e44e
SHA256值: 84d67fb1f59ee5b7cbc4781fb9d2cca585e797f1ae65db8cf14689c96f3a6c6c

i APP 信息

App名称: U蓝视频
包名: info.lkdlyb.wvd.kptr
主活动Activity:
安卓版本名称: 2.1.2
安卓版本: 212

🔍 域名线索

域名	服务器信息
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
ununtvx-1325757149.cos.ap-guangzhou.myqcloud.com	IP: 36.248.13.151 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390 经度: 119.306107
image.cnamedomain.com	没有服务器地理信息.
oss-cn-.aliyuncs.comor	没有服务器地理信息.

oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.189 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
oss.aliyuncs.com	IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
dashif.org	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
up4-intl.ucweb.com	IP: 157.185.188.1 所属国家: Canada 地区: Ontario 城市: North York 纬度: 43.771862 经度: -79.331528
up4.ucweb.com	IP: 116.132.216.194 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
opentelemetry.io	IP: 15.197.167.90 所属国家: United States of America 地区: Washington 城市: Seattle

	纬度: 47.627499 经度: -122.346199
uboyb3.cc	IP: 156.251.50.161 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
storage.googleapis.com	IP: 172.217.14.251 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
applog.uc.cn	IP: 116.132.223.75 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
ccquap0116z.bvds01f.top	没有服务器地理信息.
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

d2x4jsmvox2fim.cloudfront.net	IP: 3.165.37.198 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
gjapplog.ucweb.com	IP: 157.185.189.158 所属国家: Canada 地区: Ontario 城市: North York 纬度: 43.771862 经度: -79.331528
ns.adobe.com	没有服务器地理信息.
ap-southeast-1.log.aliyuncs.com	IP: 161.117.125.35 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
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
woodpecker.uc.cn	IP: 116.132.223.233 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
	IP: 8.138.53.74

unalyuin.oss-cn-guangzhou.aliyuncs.com	所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
wpk-auth.ucweb.com	IP: 157.185.188.1 所属国家: Canada 地区: Ontario 城市: North York 纬度: 43.771862 经度: -79.331528

 URL线索

URL信息	Url所在文件
http://dashif.org/guidelines/last-segment-number	bAZa/a08.java
http://dashif.org/guidelines/trickmode	bAZa/a08.java
https://ip.	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/OSSImpl.java
http://image.cnamedomain.com'!	com/alibaba/sdk/android/oss/OSSImpl.java
http://oss-cn-hangzhou.aliyuncs.com	com/alibaba/sdk/android/oss/common/OSSConstants.java
http://oss.aliyuncs.com	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://127.0.0.1	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://oss-cn-****.aliyuncs.com',or	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java

http://image.cnamedomain.com/!	com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java
http://%s:%d/%s	info/lexkg/vnt/nalzhc/HttpProxyCacheServer.java
https://opentelemetry.io/schemas/1.20.0	io/opentelemetry/semconv/resource/attributes/ResourceAttributes.java
https://opentelemetry.io/schemas/1.20.0	io/opentelemetry/semconv/trace/attributes/SemanticAttributes.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://github.com/danikula/AndroidVideoCache/issues/88.	jwbgi/a0v.java
https://github.com/danikula/AndroidVideoCache/issues/43.	jwbgi/a0v.java
https://github.com/danikula/AndroidVideoCache/issues.	jwbgi/a0v.java
http://%s:%d/%s	jwbgi/a1aV.java
https://github.com/danikula/AndroidVideoCache/issues/134.	jwbgi/a1aV.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	kGYlw/a08.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	kGYlw/a0M.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	kGYlw/a15.java
http://ns.adobe.com/xap/1.0/	a9lg0/a01p.java
https://gjapplog.ucweb.com/collect	FIKPD/a0v.java
https://applog.uc.cn/collect	FIKPD/a0v.java

https://wpk-auth.ucweb.com	FIKPD/a08.java
https://woodpecker.uc.cn	FIKPD/a08.java
https://up4-intl.ucweb.com/upload	FI2b/a0KjEa.java
https://up4.ucweb.com/upload	FI2b/a0KjEa.java
http://ccquap0116z.bvds01f.top/	okn9g/a0KjEa.java
http://ccquap0116z.bvds01f.top/	okn9g/a08.java
https://unalyuin.oss-cn-guangzhou.aliyuncs.com/host.jsonb	p/BQ.java
https://ununtvx-1325757149.cos.ap-guangzhou.myqcloud.com/host.jsonb	p/BQ.java
https://storage.googleapis.com/ununn5/host.jsonb	p/BQ.java
https://d2x4jsmvox2fim.cloudfront.net/host.jsonb	p/BQ.java
https://uboyb3.cc	p/BQ.java
https://t.me/uboycc01	p/BQ.java
https://ap-southeast-1.log.aliyuncs.com	LWI4u/a02Y.java
https://applog.uc.cn/collect	lib/arm64-v8a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/arm64-v8a/libcrashsdk.so
https://woodpecker.uc.cn	lib/arm64-v8a/libcrashsdk.so
https://wpk-auth.ucweb.com	lib/arm64-v8a/libcrashsdk.so

邮箱线索

邮箱地址	所在文件
danikula@gmail.com	jwbg/a0v.java

手机线索

手机号	所在文件
17512775099	cYh/a01p.java
13516237631	db2i/a08.java
17882652114	db2i/a08.java
18914945834	db2i/a08.java
16832995016	db2i/a08.java
13846158196	db2i/a08.java
17471680261	db2i/a08.java
18826691036	db2i/a08.java
14159265359	db2i/a08.java
13446589358	db2i/a08.java

19870156017	db2i/a08.java
19846674381	db2i/a08.java
17387749012	db2i/a08.java
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: False
找到 1 个唯一证书
主题: C=sevhc, ST=sevhc, L=sevhc, O=sevhc, OU=sevhc, CN=sevhc
签名算法: rsassa_pkcs1v15
有效期自: 2025-02-13 09:07:40+00:00
有效期至: 2123-09-08 09:07:40+00:00
发行人: C=sevhc, ST=sevhc, L=sevhc, O=sevhc, OU=sevhc, CN=sevhc
序列号: 0x49de1d92
哈希算法: sha256
md5值: 95d04c648d5af37525181dc4278dbbc1
sha1值: 94ee1bff2284c450f12bc2a339ef4debda7a2c8c
sha256值: 1c13bfb62f0d3af62958b9247e71dd379349b50a74955203829644327f74ac44
sha512值: 17e7ed0d173d51e212da6b448766d321a1e7f3fe891ecccfe576f8629382ae3a0f1d41b47787ceec6f4f3be78e8b32a65a563391460e0b2f0076dd3bbe686925
公钥算法: rsa
密钥长度: 3072
指纹: e692fbfddc11ae86c5960c0909c0b57a5c9ddea35d331d079fc527b67a9ccb22

🔑 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.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.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.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.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.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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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

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。