MoGua

番茄视频 2.3.6.APK 分析报告

APP名称: 番茄视频

包名:	yvy.dtwvylv.gocc
域名线索:	16条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年4月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: fqkp.apk
文件大小: 10.24MB
MD5值: d8d52fdb30126e917870bc0a2ee6fc21
SHA1值: fd0eaa1744441240146cf80e52de38d77322748c
SHA256值: 4820dff2392cde79ff70bc966f9636c9d17a95707fa667171bea520a4a852a1c

APP 信息

App名称: 番茄视频
包名: yvy.dtwvylv.gocc
主活动Activity: com.juneRain.jy.ui.activity.SplashActivity
安卓版本名称: 2.3.6
安卓版本: 16

域名线索

域名	服务器信息
errlog.umeng.com	**IP**: 223.109.148.180 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alogsus.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
ulogs.umengcloud.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu

	城市: Nanjing **纬度**: 32.061668 **经度**: 118.777992
errnewlogos.umeng.com	IP: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
errnewlog.umeng.com	IP: 223.109.148.143 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
ulogs.umeng.com	IP: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
errlogos.umeng.com	IP: 47.246.110.18 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
alogus.umeng.com	IP: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

res.openinstall.com	**IP**: 221.204.69.236 **所属国家**: China **地区**: Shanxi **城市**: Taiyuan **纬度**: 37.869438 **经度**: 112.561508
plbslog.umeng.com	**IP**: 36.156.202.68 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
43.139.150.248	**IP**: 43.139.150.248 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
aaid.umeng.com	**IP**: 223.109.148.171 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
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
pslog.umeng.com	**IP**: 59.82.29.163 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
developer.umeng.com	**IP**: 59.82.60.43 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
https://errnewlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errnewlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/d/c.java
https://43.139.150.248']	com/juneRain/jy/commonlib/channel/ChannelManager.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java

https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrashContent.java
https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrashContent.java
https://developer.umeng.com/docs/193624/detail/194590	com/umeng/umcrash/UMCrash.java
https://errnewlogos.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlogos.umeng.com	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com/upload	com/umeng/umcrash/UMCrash.java
https://errnewlog.umeng.com	com/umeng/umcrash/UMCrash.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java

https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	f1/f.java
https://res.openinstall.com/%s.dnc	io/openinstall/sdk/j.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

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=oqoedwfcwhwef, ST=idciofmsatcul, L=zkcylulualvxd, O=gbj1744014027674, OU=nxx1744014027674, CN=TG@apken888
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-07 08:20:27+00:00
有效期至: 2075-03-26 08:20:27+00:00
发行人: C=oqoedwfcwhwef, ST=idciofmsatcul, L=zkcylulualvxd, O=gbj1744014027674, OU=nxx1744014027674, CN=TG@apken888
序列号: 0x285cedc3
哈希算法: sha1
md5值: 14a5c2f0a8b7f5a492d8fb055c401065
sha1值: 19a13e0495b2c7551c7e36c0d666df31ab273797

sha256值: c8ff8bba07d60912869c73e53367e313c770483c43e97553f8f72d823a10f168
sha512值: a487f91a0752ea951d78ccc8a10a3ef0ccfc385737c32c5e1ec85f7178e6578aed65afe5901879c55630ddbfbba5f001694aacf0068ccf587ef79fbcd81736ce
公钥算法: rsa
密钥长度: 1024
指纹: e321dc13e2e43e6a54e995d1bdfbc4668dae127ab58ab924aa8f124e74854eb9

硬编码敏感信息

可能的敏感信息
"common_auth_notice_by_need_login" : "账号(ID:%s)已在其它设备登录，系统将为该设备重置全新账号"
"lunar_zodiac_monkey" : "猴"

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.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.USE_FULL_SCREEN_INTENT	正常		针对想要使用通知全屏意图的 Build.VERSION_CODES.Q 的应用程序是必需的
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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
yvy.dtwvylv.gocc_com.google.android.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
yvy.dtwvylv.gocc.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.juneRain.jy.ui.activity.SplashActivity	Schemes: h8kqpv://, um.62d11d5605844627b5ec4a4d://,