MoGua

CIBN酷视频 0.1.0.APK 分析报告

APP名称:	CIBN酷视频

包名:	cn.krcom.tv
域名线索:	26条
URL线索:	19条
邮箱线索:	0条
分析日期:	2025年5月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: CIBN酷视频.apk

文件大小: 7.38MB
MD5值: 6610d1ff8ff020fa77e8d175a79189c1
SHA1值: ca4fe8f70831a44586a2683baf33d3297d519b21
SHA256值: c75d7c527d8db257ab3a8e3637c34c584a2e764a53001db73b46efe803c0f2d6

APP 信息

App名称: CIBN酷视频
包名: cn.krcom.tv
主活动Activity: cn.krcom.tv.module.main.welcome.WelcomeActivity
安卓版本名称: 0.1.0
安卓版本: 3

域名线索

域名	服务器信息
ulogs.umengcloud.com	**IP**: 223.109.148.176 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
alogsus.umeng.com	**IP**: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
tapi.krcom.cn	**IP**: 123.125.107.13 **所属国家**: China **地区**: Beijing **城市**: Beijing

	纬度: 39.907501 **经度**: 116.397102
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
cmyip.com	没有服务器地理信息.
android.bugly.qq.com	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
tapi.cp63.ott.cibntv.net	**IP**: 123.125.107.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data.flurry.com	没有服务器地理信息.
rqd-v6.ias.tencent-cloud.net	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
rqd.sparta.mig.tencent-cloud.net	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: -

	纬度: 0.000000 **经度**: 0.000000
cmnsguider.yunos.com	IP: 203.119.175.235 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
youtube.com	IP: 199.16.158.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
dualstack-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	IP: 203.119.169.43 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
proton.flurry.com	没有服务器地理信息.
ulogs.umeng.com	IP: 223.109.148.177 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
www.cmyip.com	没有服务器地理信息.
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
developer.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
flury-ycpi.gycpi.b.yahoodns.net	**IP**: 69.147.80.15 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	**IP**: 203.119.169.41 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
alogus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992

ins-9fciednc.ias.tencent-cloud.net	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
rqd.uu.qq.com	**IP**: 60.28.219.32 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
plbslog.umeng.com	**IP**: 36.156.202.73 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
api.weibo.com	**IP**: 123.125.107.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

URL线索

URL信息	Url所在文件
http://www.cmyip.com/	cn/krcom/tv/module/main/welcome/a.java
http://tapi.cp63.ott.cibntv.net/	cn/krcom/tv/module/common/config/a.java

https://tapi.cp63.ott.cibntv.net/	cn/krcom/tv/module/common/config/a.java
https://api.weibo.com/oauth2/authorize? switch_login=1&client_id=414356030&redirect_uri=http%3a%2f%2ftapi.krcom.cn%2fresponse	cn/krcom/tv/module/common/config/a.java
http://youtube.com/yt/2012/10/10	cn/krcom/tv/player/b/b.java
https://tapi.krcom.cn	cn/krcom/b/a.java
https://data.flurry.com/pcr.do	com/flurry/sdk/aa.java
https://data.flurry.com/aap.do	com/flurry/sdk/ai.java
http://data.flurry.com/aap.do	com/flurry/sdk/ai.java
https://proton.flurry.com/sdk/v1/config	com/flurry/sdk/u.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://plbslog.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://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java

https://api.weibo.com/2/proxy/sdk/statistic.json	com/sina/weibo/sdk/statistic/e.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultPatchReporter.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultLoadReporter.java
cmyip.com	摸瓜V3引擎
flury-ycpi.gycpi.b.yahoodns.net	摸瓜V3引擎
et2-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	摸瓜V3引擎
dualstack-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com	摸瓜V3引擎
ulogs.umeng.com	摸瓜V3引擎
android.bugly.qq.com	摸瓜V3引擎
ulogs.umengcloud.com	摸瓜V3引擎
tapi.cp63.ott.cibntv.net	摸瓜V3引擎
ins-9fciednc.ias.tencent-cloud.net	摸瓜V3引擎
plbslog.umeng.com	摸瓜V3引擎
tapi.krcom.cn	摸瓜V3引擎
data.flurry.com	摸瓜V3引擎

rqd-v6.ias.tencent-cloud.net	摸瓜V3引擎
rqd.sparta.mig.tencent-cloud.net	摸瓜V3引擎
www.cmyip.com	摸瓜V3引擎

邮箱线索

手机线索

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=86, L=beijing, O=weibo, OU=weibo, CN=sina
签名算法: rsassa_pkcs1v15
有效期自: 2019-01-18 07:53:17+00:00
有效期至: 2118-12-25 07:53:17+00:00
发行人: C=86, L=beijing, O=weibo, OU=weibo, CN=sina
序列号: 0x7a71436d
哈希算法: sha256
md5值: 2fe3bf6f34b7d670ba7e9c577b794172
sha1值: 926ccc0e9f4f9e07a622971d8825d7b0757046df
sha256值: 37f1393eff6bb6f5ca16f2a9adf8bd69a10b61737233c98e079e1ae11016fe91
sha512值: abadc66595f071d25393b532b4d366922e2b1100a33a856c2966c7fb9f5d00b08a4f2d6179734fa14765db160b81c8c35d6a00c5950caa8c23c72e1f0a0709d3
公钥算法: rsa
密钥长度: 2048
指纹: 063e6a73e425c98a8c1b11e70236d9a3b841c255fb4db175d0301f1163ba1f64

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.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

		内容	
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.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.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.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.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.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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息

应用内通信