MoGua

七色猫视频 null.APK 分析报告

APP名称: 七色猫视频

包名:	com.whjzital.tmapukjh
域名线索:	16条
URL线索:	17条
邮箱线索:	4条
分析日期:	2025年9月4日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: QiSeMao.apk
文件大小: 21.86MB

MD5值: 86a2a18d567150c4d978ecad2c0a8b2a
SHA1值: 7327bb5bde6ec54a4560b1547eb6efbb2e4283cb
SHA256值: ed5ac552a5911821784d4fa2bad5989ce9a21578015b9184155997b7a980b981

APP 信息

App名称: 七色猫视频
包名: com.whjzital.tmapukjh
主活动Activity: com.wzital.tmapt.LaunchPageActivity
安卓版本名称: null
安卓版本:

域名线索

域名	服务器信息
mao-1323228439.cos.ap-nanjing.myqcloud.com	**IP**: 112.80.252.190 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
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
www.facebook.com	**IP**: 157.240.1.50 **所属国家**: United States of America **地区**: California **城市**: Menlo Park **纬度**: 37.436935 **经度**: -122.193604

ttt.xyz	**IP**: 91.195.241.232 **所属国家**: Germany **地区**: Nordrhein-Westfalen **城市**: Koeln **纬度**: 50.933346 **经度**: 6.949720
mclient.alipay.com	**IP**: 61.182.131.244 **所属国家**: China **地区**: Hebei **城市**: Zhangjiakou **纬度**: 40.810024 **经度**: 114.879349
schemas.android.com	没有服务器地理信息.
doctor.sadfate.com	没有服务器地理信息.
s3.ap-east-1.amazonaws.com	**IP**: 52.95.160.38 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
qisemao.oss-cn-nanjing.aliyuncs.com	**IP**: 47.122.12.160 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
18.162.75.251	**IP**: 18.162.75.251 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692

qisejiekou.xyz	**IP**: 16.162.214.131 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
cdn.livechatinc.com	**IP**: 23.55.47.139 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
baidu.com	**IP**: 110.242.68.66 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
qijiekou.xyz	**IP**: 16.162.214.131 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
i0.hdslb.com	**IP**: 125.39.47.217 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
plus.google.com	**IP**: 157.240.12.36 **所属国家**: Brazil **地区**: Sao Paulo **城市**: Sao Paulo **纬度**: -23.547121 **经度**: -46.637184

URL线索

URL信息	Url所在文件
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula	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/HttpProxyCacheServer.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
https://cdn.livechatinc.com/app/mobile/urls.json	com/livechatinc/inappchat/LoadWebViewContentTask.java
https://.+facebook.+(/dialog/oauth\\?	com/livechatinc/inappchat/ChatWindowView.java
https://www.facebook.com/dialog/return/arbiter	com/livechatinc/inappchat/ChatWindowView.java
https://mao-1323228439.cos.ap-nanjing.myqcloud.com/jk.json	com/wzital/tmapt/LaunchPageActivity.java

https://qisemao.oss-cn-nanjing.aliyuncs.com/jk.json	com/wzital/tmapt/LaunchPageActivity.java
https://s3.ap-east-1.amazonaws.com/ad.lmnykj.com/jk.json	com/wzital/tmapt/LaunchPageActivity.java
http://18.162.75.251	com/wzital/tmapt/LaunchPageActivity.java
https://baidu.com	com/wzital/tmapt/bean/VideoDetailInfoBean.java
https://i0.hdslb.com/bfs/archive/9312d0c09adec8023e8677eed438742620f0d430.jpg@206w_116h_1c_100q.webp	com/wzital/tmapt/home/RecommendListAdapter.java
http://doctor.sadfate.com/uploads/images/20200323/a1a3a534ac62ab56fe9231350f9c814d.gif	com/wzital/tmapt/home/RecommendListAdapter.java
https://mclient.alipay.com/h5Continue.htm?	com/wzital/tmapt/web/AlipayH5Activity.java
http://schemas.android.com/apk/res/android	j/h/a/b/c/y/g.java
https://plus.google.com/	j/h/a/b/d/k/d1.java
http://18.162.75.251	j/o/a/m0.java
https://ttt.xyz/	j/o/a/f2/b.java
https://qisejiekou.xyz/	j/o/a/f2/b.java
https://ip_host.com/	j/o/a/f2/b.java
https://qijiekou.xyz/	j/o/a/f2/b.java
https://ttt.xyz/	j/o/a/f2/j.java
https://ip_host.com/	j/o/a/f2/j.java

邮箱线索

邮箱地址	所在文件
qisemao8@gmail.com	com/wzital/tmapt/fragment/MeFragment.java
d438742620f0d430.jpg@206w_116h_1c_100q.webp	com/wzital/tmapt/home/RecommendListAdapter.java
qisemao8@gmail.com	com/wzital/tmapt/widget/CusCenterDialog.java
u0013android@android.com0 u0013android@android.com	j/h/a/b/d/u.java

手机线索

手机号	所在文件
17512775099	j/h/b/d/a.java
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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=chengdu, ST=chengdu, L=chengdu, O=nz1713240541675, OU=ay1713240541675, CN=umfm
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-16 04:09:01+00:00
有效期至: 2074-04-04 04:09:01+00:00
发行人: C=chengdu, ST=chengdu, L=chengdu, O=nz1713240541675, OU=ay1713240541675, CN=umfm
序列号: 0x7c26448e

哈希算法: sha1
md5值: 29f7dee6d145b093660fa71dc179331e
sha1值: ab8ced9d8261e29706e4fda99708a121f6267e4d
sha256值: 02d6aaaf680986fbf184ee4e35b2b373a1b99f148d1ff2004a15e0165b047459
sha512值: e62a4d3f09b12d07e821b98e07022098346f2089796c2deeec067beed68efa354c3525b35efea80a5159412fedc45793fb8c69a2f865897b1a2d61566013e65e
公钥算法: rsa
密钥长度: 1024
指纹: ba8571f7b7528973fe01a3a58389c711b6f78ba9bba93f58732177329ab2aa25

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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信