Evaluation Warning: The document was created with Spire.Doc for Python.

**狐狸视频（ 3.2版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 狐狸视频 |
| 版本 | 3.2 |
| 包名 | com.mtbook34.capp |
| 域名线索 | 46条 |
| URL线索 | 48条 |
| APP图标 |  |
| 分析日期 | 2025年5月14日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 狐狸视频.apk |
| 文件大小 | 12.6MB |
| MD5值 | f1d1f97ddf942f4430b0a5aa7209d489 |
| SHA1值 | d6314c4b024fb602fdf4ec5c182360ce62312fb1 |
| SHA256值 | 84b85b1032a241035a91f2f2a7eadb50cbe7be6b972553541054a32715ceb39d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 狐狸视频 |
| 包名 | com.mtbook34.capp |
| 主活动Activity | com.squirrel.video.ui.activity.FirstActivity |
| 安卓版本名称 | 3.2 |
| 安卓版本 | 3 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| pslog.umeng.com | IP: 59.82.60.43 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| suo.nz | IP: 42.81.120.76 所属国家: China 地区: Tianjin 城市: Tianjin  |
| schemas.android.com | 没有服务器地理信息.  |
| wspeed.qq.com | 没有服务器地理信息.  |
| pre-c.umsns.com | IP: 59.82.17.249 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing  |
| mobile.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| huatuocode.huatuo.qq.com | 没有服务器地理信息.  |
| ai.login.umeng.com | IP: 59.82.29.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Beijing 城市: Beijing  |
| www.mitaoapp.cc | IP: 172.247.103.136 所属国家: United States of America 地区: California 城市: Los Angeles  |
| developer.umeng.com | IP: 59.82.60.44 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| verify.mitaoapp.cc | 没有服务器地理信息.  |
| v3.dious.cc | IP: 137.175.8.217 所属国家: United States of America 地区: California 城市: San Jose  |
| imgcache.qq.com | IP: 119.167.203.102 所属国家: China 地区: Shandong 城市: Qingdao  |
| px.ucweb.com | IP: 106.8.139.148 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| graph.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.qplus.com | 没有服务器地理信息.  |
| appsupport.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |
| alogsus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing  |
| www.openssl.org | IP: 104.71.138.221 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| aaid.umeng.com | IP: 218.91.197.67 所属国家: China 地区: Jiangsu 城市: Nantong  |
| dev.rubaoo.com | IP: 121.43.108.235 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| qr.kegood.com | IP: 111.67.192.16 所属国家: China 地区: Beijing 城市: Beijing  |
| videoconverter.vivo.com.cn | IP: 211.93.211.94 所属国家: China 地区: Beijing 城市: Beijing  |
| log.umsns.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.unkownwebsiteblog.me | IP: 199.115.115.118 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| openmobile.qq.com | IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing  |
| vfx.mtime.cn | IP: 42.202.152.237 所属国家: China 地区: Liaoning 城市: Dalian  |
| www.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlog.umeng.com | IP: 223.109.148.142 所属国家: China 地区: Beijing 城市: Beijing  |
| rrsp-1252816746.cos.ap-shanghai.myqcloud.com | IP: 121.4.234.169 所属国家: China 地区: Beijing 城市: Beijing  |
| up.enterdesk.com | IP: 142.4.110.163 所属国家: United States of America 地区: California 城市: San Jose  |
| px-intl.ucweb.com | IP: 157.185.188.1 所属国家: United States of America 地区: California 城市: Monrovia  |
| i.loli.net | IP: 172.67.69.40 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| errlogos.umeng.com | IP: 47.246.110.96 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| c.umsns.com | IP: 59.82.31.210 所属国家: China 地区: Beijing 城市: Beijing  |
| ucc.umeng.com | IP: 203.119.169.238 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing  |
| europe.olemovienews.com | IP: 23.237.196.66 所属国家: United States of America 地区: California 城市: Los Angeles  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Beijing 城市: Beijing  |
| h.trace.qq.com | IP: 109.244.244.61 所属国家: China 地区: Beijing 城市: Beijing  |
| cgi.connect.qq.com | IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://dev.rubaoo.com/TimeDiaryV2/s/MmU5bHA=  | com/hanbing/wltc/han.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://errlogos.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://px-intl.ucweb.com  | com/uc/crashsdk/a/h.java  |
| https://px.ucweb.com  | com/uc/crashsdk/a/h.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/f/c.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/PermissionUtils.java  |
| https://www.baidu.com/  | com/squirrel/video/config/Config.java  |
| https://www.mitaoapp.cc/squirrelvideo\_config.php  | com/squirrel/video/config/Config.java  |
| http://suo.nz/api.htm?url=  | com/squirrel/video/config/Config.java  |
| http://up.enterdesk.com/edpic\_source/b3/05/f9/b305f9868c223907b60e9e7346f7fca8.jpg  | com/squirrel/video/ui/adapter/HistoryAndCollectVideoAdapter.java  |
| http://up.enterdesk.com/edpic\_source/b3/05/f9/b305f9868c223907b60e9e7346f7fca8.jpg  | com/squirrel/video/ui/adapter/VideoAdapter.java  |
| http://vfx.mtime.cn/Video/2019/03/14/mp4/190314223540373995.mp4  | com/squirrel/video/ui/activity/PlayerActivity.java  |
| http://vfx.mtime.cn/Video/2019/03/14/mp4/190314223540373995.mp4  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://i.loli.net/2021/04/18/WuAUZc85meB6D2Q.jpg  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://v3.dious.cc/20201224/6Q1yAHRu/index.m3u8  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://v3.dious.cc/20201224/aQKzuq6G/index.m3u8  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://v3.dious.cc/20201224/WWTyUxS6/index.m3u8  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| http://videoconverter.vivo.com.cn/201706/655\_1498479540118.mp4.main.m3u8  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://europe.olemovienews.com/hlstimeofffmp4/20210226/fICqcpqr/mp4/fICqcpqr.mp4/master.m3u8  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| https://rrsp-1252816746.cos.ap-shanghai.myqcloud.com/0c1f023caa3bbefbe16a5ce564142bbe.mp4  | com/squirrel/video/ui/activity/VideoDownloaderActivity.java  |
| http://qr.kegood.com/?m=0&e=L&p=5&url=  | com/squirrel/video/ui/activity/InviteActivity.java  |
| http://www.unkownwebsiteblog.me  | com/squirrel/video/ui/fragment/AgentWebFragment.java  |
| https://www.baidu.com/  | com/squirrel/video/ui/fragment/AgentWebFragment.java  |
| http://verify.mitaoapp.cc  | com/squirrel/video/helper/UserHttpHelper.java  |
| http://verify.mitaoapp.cc/?r=cdk/isVip&deviceId=  | com/squirrel/video/helper/UserHttpHelper.java  |
| http://verify.mitaoapp.cc/?r=cdk/addVip&deviceId=  | com/squirrel/video/helper/UserHttpHelper.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.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://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://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/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  |
| http://log.umsns.com/link/qq/download/  | com/umeng/socialize/handler/QZoneSsoHandler.java  |
| https://graph.qq.com/oauth2.0/me?access\_token=  | com/umeng/socialize/handler/UMQQSsoHandler.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/socialize/utils/UrlUtil.java  |
| https://log.umsns.com/  | com/umeng/socialize/view/OauthDialog.java  |
| https://log.umsns.com/  | com/umeng/socialize/common/SocializeConstants.java  |
| https://log.umsns.com/link/qq/download/  | com/umeng/socialize/common/SocializeConstants.java  |
| https://log.umsns.com/link/weixin/download/  | com/umeng/socialize/common/SocializeConstants.java  |
| http://www.umeng.com/social  | com/umeng/socialize/common/SocializeConstants.java  |
| https://c.umsns.com/ulink/getRTC  | com/umeng/socialize/tracker/a.java  |
| https://pre-c.umsns.com/ulink/getRTC  | com/umeng/socialize/tracker/a.java  |
| https://mobile.umeng.com/images/pic/home/social/img-1.png  | com/umeng/socialize/net/LinkcardRequest.java  |
| https://log.umsns.com/  | com/umeng/socialize/net/base/SocializeRequest.java  |
| https://ai.login.umeng.com/api/umed/event  | com/umeng/socialize/net/analytics/SocialAnalytics.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/UMRemoteConfig.java  |
| https://ucc.umeng.com/v1/fetch  | com/umeng/cconfig/c/b.java  |
| https://pslog.umeng.com/ablog  | com/umeng/cconfig/c/b.java  |
| https://openmobile.qq.com/oauth2.0/me  | com/tencent/connect/UnionInfo.java  |
| https://openmobile.qq.com/oauth2.0/m\_jump\_by\_version?  | com/tencent/connect/common/BaseApi.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/common/BaseApi.java  |
| https://openmobile.qq.com/oauth2.0/m\_authorize?  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/user/user\_login\_statis  | com/tencent/connect/auth/AuthAgent.java  |
| https://openmobile.qq.com/v3/user/get\_info  | com/tencent/connect/auth/AuthAgent.java  |
| https://appsupport.qq.com/cgi-bin/qzapps/mapp\_addapp.cgi  | com/tencent/connect/auth/AuthAgent.java  |
| https://imgcache.qq.com/ptlogin/static/qzsjump.html?  | com/tencent/connect/auth/a.java  |
| https://cgi.qplus.com/report/report  | com/tencent/connect/avatar/ImageActivity.java  |
| https://imgcache.qq.com/open/mobile/request/sdk\_request.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/invite/sdk\_invite.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com/open/mobile/sendstory/sdk\_sendstory\_v1.3.html?  | com/tencent/open/SocialApiIml.java  |
| https://imgcache.qq.com  | com/tencent/open/SocialApiIml.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/unbind  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/cgi-bin/qunopensdk/check\_group  | com/tencent/open/SocialOperation.java  |
| https://openmobile.qq.com/  | com/tencent/open/utils/HttpUtils.java  |
| https://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf  | com/tencent/open/utils/g.java  |
| https://wspeed.qq.com/w.cgi  | com/tencent/open/b/h.java  |
| https://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report  | com/tencent/open/b/h.java  |
| https://huatuocode.huatuo.qq.com  | com/tencent/open/b/e.java  |
| https://h.trace.qq.com/kv  | com/tencent/open/b/b.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 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**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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.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.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\_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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent101973610://,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**