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

**猫影视（ 1.1.0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 | 猫影视 |
| 版本 | 1.1.0 |
| 包名 | com.github.catvod.app |
| 域名线索 | 29条 |
| URL线索 | 10条 |
| APP图标 |  |
| 分析日期 | 2024年9月17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 | android\_open\_1.1.0\_fix1.apk |
| 文件大小 | 32.26MB |
| MD5值 | a987c7bc107da066b0cd7392dda22f50 |
| SHA1值 | 0dac0b9aff5b1ba690a9541c39a56d60b9f142a5 |
| SHA256值 | 576aae978461ac95a64fc852f7b61b4b3cea65f994b4df362ea3eacc717d6c5d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 猫影视 |
| 包名 | com.github.catvod.app |
| 主活动Activity | com.github.catvod.app.MainActivity |
| 安卓版本名称 | 1.1.0 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| alist.xiaoya.pro | IP: 172.67.178.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| alist.shenzjd.com | IP: 106.55.242.160 所属国家: China 地区: Beijing 城市: Beijing  |
| movie.douban.com | IP: 49.233.242.15 所属国家: China 地区: Beijing 城市: Beijing  |
| dashif.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| pan.bashroot.top | IP: 172.67.148.175 所属国家: United States of America 地区: California 城市: San Francisco  |
| mozilla.github.io | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| search.video.iqiyi.com | IP: 123.126.131.94 所属国家: China 地区: Beijing 城市: Beijing  |
| v1.jinrishici.com | IP: 119.249.102.35 所属国家: China 地区: Hebei 城市: Baoding  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| pan.xwbeta.com | IP: 124.220.233.93 所属国家: China 地区: Beijing 城市: Beijing  |
| pan.jlbx.xyz | IP: 172.67.217.125 所属国家: United States of America 地区: California 城市: San Francisco  |
| al.chirmyram.com | IP: 104.21.77.26 所属国家: United States of America 地区: California 城市: San Francisco  |
| node.video.qq.com | IP: 60.28.172.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| alist.youte.ml | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ali.liucn.repl.co | IP: 35.186.245.55 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| api.web.360kan.com | IP: 101.199.255.49 所属国家: China 地区: Beijing 城市: Beijing  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| developer.android.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| npms.io | IP: 104.21.49.221 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.360kan.com | IP: 111.161.122.18 所属国家: China 地区: Tianjin 城市: Tianjin  |
| api.github.com | IP: 20.205.243.168 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.ibm.com | IP: 2.18.159.141 所属国家: France 地区: Ile-de-France 城市: Paris  |
| gitee.com | IP: 180.76.198.77 所属国家: China 地区: Beijing 城市: Beijing  |
| 110.42.2.115 | IP: 110.42.2.115 所属国家: China 地区: Zhejiang 城市: Ningbo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/i.java  |
| http://alist.xiaoya.pro/  | Mogua Engine V2  |
| https://alist.youte.ml  | Mogua Engine V2  |
| https://al.chirmyram.com  | Mogua Engine V2  |
| https://alist.shenzjd.com  | Mogua Engine V2  |
| https://pan.jlbx.xyz  | Mogua Engine V2  |
| https://pan.bashroot.top  | Mogua Engine V2  |
| https://ali.liucn.repl.co  | Mogua Engine V2  |
| https://pan.xwbeta.com  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml  | Mogua Engine V2  |
| http://www.w3.org/1998/Math/MathML  | Mogua Engine V2  |
| http://www.w3.org/2000/svg  | Mogua Engine V2  |
| http://www.w3.org/1999/xlink  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/  | Mogua Engine V2  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | Mogua Engine V2  |
| http://'+n+'  | Mogua Engine V2  |
| http://mozilla.github.io/nunjucks/api.html  | Mogua Engine V2  |
| https://npms.io/search?q=ponyfill.  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/libflutter.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/libflutter.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| http://www.smpte-ra.org/schemas/2067-3/2013  | lib/arm64-v8a/libmpv.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/libmpv.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/arm64-v8a/libmpv.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/libmpv.so  |
| http://110.42.2.115:880/analysis/json/?uid=2100&my=abhstwDGRSUVYZ0127&mgtv=app&url=https://www.iqiyi.com/v\_21o4h97oys4.html  | lib/armeabi-v7a/libapp.so  |
| https://node.video.qq.com/x/api/hot\_search  | lib/armeabi-v7a/libapp.so  |
| https://api.github.com/repos/  | lib/armeabi-v7a/libapp.so  |
| https://gitee.com/api/v5/repos/  | lib/armeabi-v7a/libapp.so  |
| http://127.0.0.1:  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| https://api.web.360kan.com/v1/rank?cat=  | lib/armeabi-v7a/libapp.so  |
| https://www.360kan.com/rank/general  | lib/armeabi-v7a/libapp.so  |
| https://search.video.iqiyi.com/m  | lib/armeabi-v7a/libapp.so  |
| https://movie.douban.com/  | lib/armeabi-v7a/libapp.so  |
| https://v1.jinrishici.com/all  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/XML/1998/namespace  | lib/armeabi-v7a/libflutter.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libflutter.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| http://www.smpte-ra.org/schemas/2067-3/2013  | lib/armeabi-v7a/libmpv.so  |
| http://www.w3.org/XML/1998/namespace  | lib/armeabi-v7a/libmpv.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/armeabi-v7a/libmpv.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libmpv.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| \_typeerror@0150898.\_create \_double@0150898.fromintege \_growablelist@0150898.\_literal \_immutablelist@0150898.\_fl \_bytebuffer@7027147.\_new \_casterror@0150898.\_create \_assertionerror@0150898.\_create  | lib/armeabi-v7a/libapp.so  |

### **4.4 手机号线索**

## **5. 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=CN, ST=HF, L=HF, O=WorkGroup, OU=WorkGroup, CN=Simon.H 签名算法: rsassa\_pkcs1v15 有效期自: 2018-01-08 07:25:11+00:00 有效期至: 2068-01-08 07:25:11+00:00 发行人: C=CN, ST=HF, L=HF, O=WorkGroup, OU=WorkGroup, CN=Simon.H 序列号: 0x5a531cd7 哈希算法: sha256 md5值: ae020f45ed0016a6449f48a8e68a313a sha1值: 0571dc346170be17d6fafa49f09c7491a7ec9b15 sha256值: ba83e379409e35186f513d3a65c9b671f4cfa96ec957b7c0448710c14ec6dcbe sha512值: 8a07201a4f29359a8848948ab7db4cad02744e45ae4e475594938d3ff3c063f5e13856a5584f2f18a1cc815fcf67244c5ecdf299a41fd87b3376a53e4e15cd9a 公钥算法: rsa 密钥长度: 2048 指纹: 5273b92e9421fae56a92b7a79b70ee1bfb044509e82d08f29c7bfd827dc6e7c5**

## **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.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 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |

## **10. 应用内通信**

**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。**