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

**色狐（ 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 | 色狐 |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 33条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2024年9月19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 | sehu-p8YiC-v1018523.apk |
| 文件大小 | 33.33MB |
| MD5值 | 1f79cf7f0f52efa62bf9abb9a1e20781 |
| SHA1值 | 79914acaa8b236c45865d38cbb4968d64a7b404f |
| SHA256值 | 8092a9421945976f070598262021cde9479b4eb734a9e3ce5e298943bebc50a8 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 色狐 |
| 包名 |  |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | [] |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| r.photo.store.qq.com | IP: 182.50.15.121 所属国家: China 地区: Beijing 城市: Beijing  |
| speedtestint.trtc.tencent-cloud.com | IP: 43.156.222.141 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| intl-sdklog.trtc.tencent-cloud.com | IP: 43.156.222.59 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| cloud.tencent.com | IP: 61.49.23.183 所属国家: China 地区: Beijing 城市: Beijing  |
| videoapi-sgp.im.qcloud.com | IP: 124.64.207.114 所属国家: China 地区: Beijing 城市: Beijing  |
| flvmock.tencent.com | 没有服务器地理信息.  |
| test.tim.qq.com | IP: 106.55.123.101 所属国家: China 地区: Beijing 城市: Beijing  |
| sdkdc.live.qcloud.com | IP: 43.153.127.15 所属国家: United States of America 地区: California 城市: Santa Clara  |
| speedtest.trtc.tencent-cloud.com | IP: 162.14.6.106 所属国家: China 地区: Beijing 城市: Beijing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| trtc-sdk-config-1258344699.file.myqcloud.com | IP: 119.167.147.251 所属国家: China 地区: Shandong 城市: Qingdao  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| trtc-client-log-overseas-1258344699.cos.ap-singapore.myqcloud.com | IP: 43.128.240.46 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| livepullipv6.myqcloud.com | IP: 163.177.30.38 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| common-proxy.rtc.tencent.com | IP: 106.55.209.148 所属国家: China 地区: Beijing 城市: Beijing  |
| tcdnsipv6.myqcloud.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| 106.55.123.30 | IP: 106.55.123.30 所属国家: China 地区: Beijing 城市: Beijing  |
| avmonitortest.trtc.tencent-cloud.com | IP: 106.53.137.253 所属国家: China 地区: Beijing 城市: Beijing  |
| inland-sdklog.trtc.tencent-cloud.com | IP: 120.53.64.22 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| tcdns.myqcloud.com | IP: 109.244.168.67 所属国家: China 地区: Beijing 城市: Beijing  |
| livepull.myqcloud.com | IP: 116.130.223.85 所属国家: China 地区: Beijing 城市: Beijing  |
| liteav.sdk.qcloud.com | IP: 110.249.196.62 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| mlvbdc.live.qcloud.com | IP: 153.3.149.192 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| trtc-sdk-log-1258344699.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.173 所属国家: China 地区: Fujian 城市: Fuzhou  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| common-proxyintl.rtc.tencent.com | IP: 43.156.255.121 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| conf.sdk.qcloud.com | IP: 43.137.144.90 所属国家: China 地区: Beijing 城市: Beijing  |
| yun.tim.qq.com | IP: 60.29.232.105 所属国家: China 地区: Tianjin 城市: Tianjin  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| common-proxy-test.rtc.tencent.com | IP: 175.27.204.228 所属国家: China 地区: Beijing 城市: Beijing  |
| ns.adobe.com | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| http://r.photo.store.qq.com/psb?/V14dALyK4PrHuj/ch4tK\*lEnQ3CzEK726Mw6AJFG\*DX\*t3aYQZOUI0c0VA!/r/dMMAAAAAAAAA  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |
| http://kiwi\_live/tunnel/a033b072?z=1&nobase64=1  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| http://127.0.0.1:%d/proxy/%d/%d/vod\_%d.m3u8?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/%s?play\_id=%d&clip\_id=%d&force\_online=0%s  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/master.m3u8?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/vod.mp4?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/%s\_tp\_dl\_autotype?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/%s?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/vod.m3u8?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/live.m3u8?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/1/%s.flv?play\_id=%d&clip\_id=1&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.so  |
| http://127.0.0.1:%d/proxy/%d/%d/loop.m3u8?play\_id=%d&clip\_id=%d&force\_online=0  | lib/armeabi-v7a/libdownloadproxy.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://ns.adobe.com/xap/1.0/  | lib/armeabi-v7a/libimagepipeline.so  |
| https://sdkdc.live.qcloud.com/liteav  | lib/armeabi-v7a/libliteavsdk.so  |
| https://mlvbdc.live.qcloud.com/liteav  | lib/armeabi-v7a/libliteavsdk.so  |
| https://intl-sdklog.trtc.tencent-cloud.com/log/report  | lib/armeabi-v7a/libliteavsdk.so  |
| https://inland-sdklog.trtc.tencent-cloud.com/log/report  | lib/armeabi-v7a/libliteavsdk.so  |
| https://106.55.123.30/rainbowapi.configs/getdatas  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-sdk-config-1258344699.file.myqcloud.com/liteavsvrcfg/v3/serverconfig\_enc.zip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://liteav.sdk.qcloud.com/sdkres/config/v2/serverconfig\_enc.zip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://intl-sdklog.trtc.tencent-cloud.com/log/appsign  | lib/armeabi-v7a/libliteavsdk.so  |
| https://inland-sdklog.trtc.tencent-cloud.com/log/appsign  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxy.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxy-test.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://common-proxyintl.rtc.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://test.tim.qq.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://yun.tim.qq.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-sdk-log-1258344699.cos.ap-guangzhou.myqcloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://trtc-client-log-overseas-1258344699.cos.ap-singapore.myqcloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://videoapi-sgp.im.qcloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://speedtest.trtc.tencent-cloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://speedtestint.trtc.tencent-cloud.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://avmonitortest.trtc.tencent-cloud.com:8000  | lib/armeabi-v7a/libliteavsdk.so  |
| http://flvmock.tencent.com  | lib/armeabi-v7a/libliteavsdk.so  |
| https://cloud.tencent.com/document/product/454/56598  | lib/armeabi-v7a/libliteavsdk.so  |
| https://conf.sdk.qcloud.com/rainbowapi.configs/getdatas  | lib/armeabi-v7a/libliteavsdk.so  |
| https://tcdns.myqcloud.com/queryip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://tcdnsipv6.myqcloud.com/queryip  | lib/armeabi-v7a/libliteavsdk.so  |
| https://livepull.myqcloud.com/getpulladdr  | lib/armeabi-v7a/libliteavsdk.so  |
| https://livepullipv6.myqcloud.com/getpulladdr  | lib/armeabi-v7a/libliteavsdk.so  |
| http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip><track\_clip><clip\_id>15</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593478281.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2000</clip\_endTimeMs><clip\_playTimeMs>2000</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip></video\_track></video\_tracks><audio\_tracks><audio\_track><track\_id>1</track\_id><track\_clip><clip\_id>18</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593473438.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2206</clip\_endTimeMs><clip\_playTimeMs>2206</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip><track\_clip><clip\_id>19</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593478281.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>1950</clip\_endTimeMs><clip\_playTimeMs>1950</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip></audio\_track><audio\_track><track\_id>2</track\_id><track\_clip><clip\_id>20</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/Android/data/com.tencent.qqlive/files/mediaDownload/s0026hgpb92.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>4200</clip\_endTimeMs><clip\_playTimeMs>4200</clip\_playTimeMs><clip\_loop>0</clip\_loop><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip></audio\_track></audio\_tracks><av\_tracks><av\_track><track\_id>1</track\_id><track\_clip><clip\_id>18</clip\_id><clip\_placeHolder>0</clip\_placeHolder><clip\_path><![CDATA[/storage/emulated/0/tencent/TencentVideo/CameraRecord/record\_1527593473438.mp4]]></clip\_path><clip\_durationMs>30000</clip\_durationMs><clip\_startTimeMs>0</clip\_startTimeMs><clip\_endTimeMs>2206</clip\_endTimeMs><clip\_playTimeMs>2206</clip\_playTimeMs><clip\_drmType>0</clip\_drmType><clip\_drmProvisionUrl><![CDATA[http://drmProvisionUrl]]></clip\_drmProvisionUrl><clip\_drmLicenseUrl><![CDATA[http://drmLicenseUrl]]></clip\_drmLicenseUrl><clip\_drmUseL1>1</clip\_drmUseL1><clip\_drmSavePath><![CDATA[/sdcard/]]></clip\_drmSavePath><clip\_drmGuid><![CDATA[guid]]></clip\_drmGuid><clip\_drmPlatform><![CDATA[platform]]></clip\_drmPlatform><clip\_drmAppVersion><![CDATA[appVersion]]></clip\_drmAppVersion><clip\_drmCookie><![CDATA[cookie]]></clip\_drmCookie><clip\_drmExtXKey><![CDATA[drmExtXKey]]></clip\_drmExtXKey></track\_clip></av\_track></av\_tracks></assets>  | lib/armeabi-v7a/libtpcore-master.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| \_httpparser@13463476.responsepa .\_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat c\_growablelist@0150898.withcapaci \_receiveportimpl@1026248.fromrawrec m\_growablelist@0150898.\_literal2 g\_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_colorfilter@16065589.srgbtoline q\_imagefilter@16065589.blur \_growablelist@0150898.\_literal4 x\_growablelist@0150898.of k\_colorfilter@16065589.lineartosr \_list@0150898.of \_list@0150898.generate n\_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_socket@14069316.\_readpipe \_list@0150898.\_ofother eo\_bytebuffer@7027147.\_new storationinformation@771124995.fromserial av\_nativesocket@14069316.normal j\_filestream@14069316.forstdin qd\_growablelist@0150898.\_literal8 lectiontoolbarbutton@372392285.text lectiontoolbarbutton@495113492.text \_future@4048458.zonevalue \_double@0150898.fromintege \_growablelist@0150898.\_literal6 -\_list@0150898.\_ofarray z\_timer@1026248.periodic \_casterror@0150898.\_create l\_invocationmirror@0150898.\_withtype \_colorfilter@16065589.mode i\_rawsocket@14069316.\_writepipe \_growablelist@0150898.\_literal1 4\_uri@0150898.file bb\_growablelist@0150898.\_ofgrowabl \_nativesocket@14069316.pipe \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_growablelist@0150898.\_literal3 u\_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_uri@0150898.directory v\_file@14069316.fromrawpat gh\_growablelist@0150898.generate \_uri@0150898.notsimple 7u\_growablelist@0150898.\_literal7 \_\_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14410538052  | lib/armeabi-v7a/libapp.so  |

## **5. 签名证书**

**无法读取代码签名证书.**

## **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**

## **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。**