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

**久赢恒丰（ 1.3.6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 | 久赢恒丰 |
| 版本 | 1.3.6 |
| 包名 | com.txcf.cronuss |
| 域名线索 | 72条 |
| URL线索 | 43条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | base.apk |
| 文件大小 | 144.17MB |
| MD5值 | f7dd58113ded10761330aa3ab465b168 |
| SHA1值 | dc5c72fb8119e68641915125207ef7fcce496b4f |
| SHA256值 | 26e9fb783f91b686fef9501e2faf8d68d3c8341d6b803a2317ebd83ef07c0793 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 久赢恒丰 |
| 包名 | com.txcf.cronuss |
| 主活动Activity | com.txcf.cronuss.MainActivity |
| 安卓版本名称 | 1.3.6 |
| 安卓版本 | 10306 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| loggw-exsdk.alipay.com | IP: 110.76.6.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.example.com | IP: 125.56.201.98 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dns.alidns.com | IP: 223.6.6.6 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| umc.danuoyi.alicdn.com | IP: 101.37.12.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| gw.rtn.aliyuncs.com | IP: 60.205.93.126 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| vpp-license-proxy.aliyuncs.com | IP: 106.15.100.116 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mcgw.alipay.com | IP: 123.125.216.191 所属国家: China 地区: Beijing 城市: Beijing  |
| cn.register.xmpush.xiaomi.com | IP: 123.125.102.39 所属国家: China 地区: Beijing 城市: Beijing  |
| work.weixin.qq.com | IP: 106.55.127.35 所属国家: China 地区: Beijing 城市: Beijing  |
| www.alibaba.com | IP: 203.119.238.116 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| beian.miit.gov.cn | IP: 119.39.205.85 所属国家: China 地区: Hunan 城市: Zhuzhou  |
| alivc-player.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.65 所属国家: China 地区: Shanghai 城市: Shanghai  |
| cloud-config-service-pre.rtc.aliyuncs.com | IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wappaygw.alipay.com | IP: 123.125.216.192 所属国家: China 地区: Beijing 城市: Beijing  |
| metrics5.dt.dbankcloud.ru | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| render.alipay.com | IP: 221.207.101.98 所属国家: China 地区: Heilongjiang 城市: Jiamusi  |
| slsrole.alicdn.com | IP: 218.11.15.235 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| cloud-config-service.rtc.aliyuncs.com | IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics1-drcn.dt.dbankcloud.cn | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| log-global-cn-shenzhen.aliyuncs.com | 没有服务器地理信息.  |
| 10.38.162.35 | IP: 10.38.162.35 所属国家: - 地区: - 城市: -  |
| schemas.android.com | 没有服务器地理信息.  |
| app.txcfgl.com | IP: 47.99.190.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| mobilegwpre.alipay.com | IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 116.128.169.212 所属国家: China 地区: Shanghai 城市: Shanghai  |
| www.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| miniapp.guniuniu.com | IP: 47.99.190.68 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| purl.org | IP: 207.241.225.157 所属国家: United States of America 地区: California 城市: San Francisco  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| mclient.alipay.com | IP: 1.28.232.212 所属国家: China 地区: Nei Mongol 城市: Baotou  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| vod-license-proxy-pre.aliyun-inc.com | IP: 100.64.26.218 所属国家: - 地区: - 城市: -  |
| ns.adobe.com | 没有服务器地理信息.  |
| pgw.rtn.aliyuncs.com | IP: 47.93.47.144 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| resolver.msg.xiaomi.net | IP: 39.102.218.17 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| help.aliyun.com | IP: 203.119.144.7 所属国家: China 地区: Beijing 城市: Beijing  |
| live.aliyuncs.com | IP: 59.82.44.229 所属国家: China 地区: Shanghai 城市: Shanghai  |
| vod-license.cn-shanghai.aliyuncs.com | IP: 8.139.73.64 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| data-drcn.push.dbankcloud.com | IP: 118.194.33.160 所属国家: China 地区: Shanghai 城市: Shanghai  |
| dartbug.com | IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.webrtc.org | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.alibabacloud.com | IP: 47.241.205.194 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mobilegw.dl.alipaydev.com | IP: 110.75.132.25 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.ibm.com | IP: 23.59.2.229 所属国家: Japan 地区: Osaka 城市: Ibaraki  |
| mobilegw.alipay.com | IP: 203.209.243.98 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mp.weixin.qq.com | IP: 220.196.132.78 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| h5.m.taobao.com | IP: 125.38.11.130 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cn-hangzhou.log.aliyuncs.com | IP: 47.114.236.51 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| videocloud.cn-hangzhou.log.aliyuncs.com | IP: 47.96.32.228 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| developer.android.com | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| vpp-license-proxy.taobao.net | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.example.com  | a0/e.java  |
| https://mobilegwpre.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| https://help.aliyun.com/zh/live/developer-reference/integrate-a-push-sdk-license  | com/alivc/live/pusher/basic/AlivcBasicLivePusherImpl.java  |
| https://help.aliyun.com/zh/live/developer-reference/integrate-a-push-sdk-license  | com/alivc/live/pusher/rtc/AlivcRTCLivePusherImpl.java  |
| https://videocloud.cn-hangzhou.log.aliyuncs.com/logstores/  | com/alivc/live/biz/logreport/core/c.java  |
| https://help.aliyun.com/zh/live/developer-reference/integrate-a-push-sdk-license\n  | com/alivc/live/biz/manager/b.java  |
| https://help.aliyun.com/zh/apsara-video-sdk/user-guide/license/\n  | com/alivc/live/biz/manager/b.java  |
| https://www.alibabacloud.com/help/en/live/developer-reference/integrate-a-push-sdk-license\n  | com/alivc/live/biz/manager/b.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/c.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/b.java  |
| https://mp.weixin.qq.com/publicpoc/opensdkconf?action=GetShareConf&appid=%s&sdkVersion=%s&buffer=%s  | com/tencent/mm/opensdk/openapi/WXAPiSecurityHelper.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gv.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/hn.java  |
| https://%1$s/gslb/?ver=5.0  | com/xiaomi/push/dc.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ho.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gj.java  |
| http://10.38.162.35:9085  | com/xiaomi/push/service/w.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/w.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bx.java  |
| https://developer.android.com/guide/topics/permissions/overview  | fe/f.java  |
| http://schemas.android.com/apk/res/android  | o0/p.java  |
| https://mobilegw.alipay.com/mgw.htm  | o4/a.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | o4/a.java  |
| https://mobilegw.dl.alipaydev.com/mgw.htm  | o4/a.java  |
| https://mcgw.alipay.com/sdklog.do  | o4/a.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | o4/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | o4/a.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | o4/a.java  |
| https://render.alipay.com/p/s/i?scheme=%s  | q3/b.java  |
| https://docs.flutter.dev/deployment/android  | pd/f.java  |
| https://github.com/flutter/packages/blob/main/packages/in\_app\_purchase/in\_app\_purchase/README.md  | xe/j.java  |
| http://dashif.org/guidelines/last-segment-number  | v9/d.java  |
| http://dashif.org/guidelines/trickmode  | v9/d.java  |
| http://dashif.org/thumbnail\_tile  | v9/d.java  |
| http://dashif.org/guidelines/thumbnail\_tile  | v9/d.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | y1/a.java  |
| http://ns.adobe.com/xap/1.0/  | x8/a.java  |
| https://h5.m.taobao.com/mlapp/olist.html  | q4/a.java  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://metrics1-drcn.dt.dbankcloud.cn:443  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.dt.dbankcloud.ru:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v3/getLivePushConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| http://%s/multi\_httpdns\_resolve?qtype=a&host\_key=%.200s  | lib/arm64-v8a/liball\_in\_one.so  |
| http://%s/multi\_httpdns\_resolve?qtype=aaaa&host\_key=%.200s  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cn-hangzhou.log.aliyuncs.com  | lib/arm64-v8a/liball\_in\_one.so  |
| https://help.aliyun.com/document\_detail/434250.html'  | lib/arm64-v8a/liball\_in\_one.so  |
| https://help.aliyun.com/document\_detail/52841.html  | lib/arm64-v8a/liball\_in\_one.so  |
| https://help.aliyun.com/zh/apsara-video-sdk/user-guide/license/'  | lib/arm64-v8a/liball\_in\_one.so  |
| http://vpp-license-proxy.taobao.net/  | lib/arm64-v8a/liball\_in\_one.so  |
| https://vod-license-proxy-pre.aliyun-inc.com/  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cloud-config-service-pre.rtc.aliyuncs.com/configservice/v1/getPlayerConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getPlayerConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| https://vod.  | lib/arm64-v8a/liball\_in\_one.so  |
| https://live.aliyuncs.com/  | lib/arm64-v8a/liball\_in\_one.so  |
| https://live.  | lib/arm64-v8a/liball\_in\_one.so  |
| https://mts.  | lib/arm64-v8a/liball\_in\_one.so  |
| https://videocloud.cn-hangzhou.log.aliyuncs.com/logstores/newplayer/track  | lib/arm64-v8a/liball\_in\_one.so  |
| http://xxx  | lib/arm64-v8a/liball\_in\_one.so  |
| https://dns.alidns.com/resolve  | lib/arm64-v8a/liball\_in\_one.so  |
| http://umc.danuoyi.alicdn.com/dns\_resolve\_backup?host\_key=  | lib/arm64-v8a/liball\_in\_one.so  |
| https://alivc-player.oss-cn-shanghai.aliyuncs.com/playerTest/  | lib/arm64-v8a/liball\_in\_one.so  |
| https://pgw.rtn.aliyuncs.com  | lib/arm64-v8a/liball\_in\_one.so  |
| https://gw.rtn.aliyuncs.com  | lib/arm64-v8a/liball\_in\_one.so  |
| https://slsrole.alicdn.com  | lib/arm64-v8a/liball\_in\_one.so  |
| http://log-global-cn-shenzhen.aliyuncs.com  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cloud-config-service-pre.rtc.aliyuncs.com/configservice/v1/getRtcRawUrlConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getRtcRawUrlConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getAioLoggerConfig  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/media\_extension\_data  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/decoding-timestamp  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/audio\_ranking\_level\_id  | lib/arm64-v8a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/picture\_id  | lib/arm64-v8a/liball\_in\_one.so  |
| https://vpp-license-proxy.taobao.net/auth  | lib/arm64-v8a/liball\_in\_one.so  |
| https://vod-license-proxy-pre.aliyun-inc.com/auth  | lib/arm64-v8a/liball\_in\_one.so  |
| https://vpp-license-proxy.aliyuncs.com/auth  | lib/arm64-v8a/liball\_in\_one.so  |
| http://vod-license.cn-shanghai.aliyuncs.com/auth  | lib/arm64-v8a/liball\_in\_one.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v3/getLivePushConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://%s/multi\_httpdns\_resolve?qtype=a&host\_key=%.200s  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://%s/multi\_httpdns\_resolve?qtype=aaaa&host\_key=%.200s  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cn-hangzhou.log.aliyuncs.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://help.aliyun.com/document\_detail/434250.html'  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://help.aliyun.com/document\_detail/52841.html  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://help.aliyun.com/zh/apsara-video-sdk/user-guide/license/'  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://vpp-license-proxy.taobao.net/  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://vod-license-proxy-pre.aliyun-inc.com/  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cloud-config-service-pre.rtc.aliyuncs.com/configservice/v1/getPlayerConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getPlayerConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://vod.  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://live.aliyuncs.com/  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://live.  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://mts.  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://videocloud.cn-hangzhou.log.aliyuncs.com/logstores/newplayer/track  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://xxx  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://dns.alidns.com/resolve  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://umc.danuoyi.alicdn.com/dns\_resolve\_backup?host\_key=  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://alivc-player.oss-cn-shanghai.aliyuncs.com/playerTest/  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://pgw.rtn.aliyuncs.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://gw.rtn.aliyuncs.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://slsrole.alicdn.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://log-global-cn-shenzhen.aliyuncs.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cloud-config-service-pre.rtc.aliyuncs.com/configservice/v1/getRtcRawUrlConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getRtcRawUrlConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://cloud-config-service.rtc.aliyuncs.com/configservice/v1/getAioLoggerConfig  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/media\_extension\_data  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/decoding-timestamp  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/audio\_ranking\_level\_id  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://www.alibaba.com/experiments/rtp-hdrext/picture\_id  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://vpp-license-proxy.taobao.net/auth  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://vod-license-proxy-pre.aliyun-inc.com/auth  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://vpp-license-proxy.aliyuncs.com/auth  | lib/armeabi-v7a/liball\_in\_one.so  |
| http://vod-license.cn-shanghai.aliyuncs.com/auth  | lib/armeabi-v7a/liball\_in\_one.so  |
| https://miniapp.guniuniu.com/agreement.html  | lib/armeabi-v7a/libapp.so  |
| https://app.txcfgl.com  | lib/armeabi-v7a/libapp.so  |
| https://miniapp.guniuniu.com/h5/  | lib/armeabi-v7a/libapp.so  |
| http://ns.adobe.com/xfdf/  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| http://purl.org/dc/elements/1.1/  | lib/armeabi-v7a/libapp.so  |
| https://miniapp.guniuniu.com/privacy.html  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://github.com/dart-lang/language/issues/3488  | lib/armeabi-v7a/libapp.so  |
| https://work.weixin.qq.com/ca/cawcde2d8257505bad  | lib/armeabi-v7a/libapp.so  |
| https://beian.miit.gov.cn/  | lib/armeabi-v7a/libapp.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| https://app.txcfgl.com/api  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/x86\_64/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/x86\_64/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/x86\_64/libflutter.so  |
| https://dartbug.com/52121.  | lib/x86\_64/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/arm64-v8a/liball\_in\_one.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| ftp@example.com  | lib/armeabi-v7a/liball\_in\_one.so  |
| \_httpparser@13463476.responsepa storationinformation@153124995.fromserial \_internetaddress@14069316.fixed \_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_receiveportimpl@1026248.fromrawrec \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_colorfilter@15065589.lineartosr \_growablelist@0150898.\_literal4 \_growablelist@0150898.of \_list@0150898.of \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_future@4048458.value \_list@0150898.\_ofother \_bytebuffer@7027147.\_new \_nativesocket@14069316.normal \_colorfilter@15065589.srgbtoline \_growablelist@0150898.\_literal8 \_future@4048458.zonevalue \_nativesocket@14069316.listen \_pointerpanzoomdata@296213599.fromupdate \_double@0150898.fromintege \_growablelist@0150898.\_literal6 \_colorfilter@15065589.mode \_imagefilter@15065589.composed \_list@0150898.\_ofarray \_timer@1026248.periodic \_compressednode@54137193.single \_invocationmirror@0150898.\_withtype \_assetmanifestbin@62287047.fromstanda \_growablelist@0150898.\_literal1 \_uri@0150898.file \_imagefilter@15065589.blur \_growablelist@0150898.\_ofgrowabl authenticationscheme@13463476.fromstring \_hashcollisionnode@54137193.fromcollis \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_imagefilter@15065589.fromcolorf \_uri@0150898.directory \_httpparser@13463476.requestpar \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |
| appro@openssl.org  | lib/x86\_64/libflutter.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15724800000  | cn/jiguang/am/a.java  |
| 17512775099  | ib/b.java  |
| 18222222222  | y8/e.java  |
| 15838186836  | 摸瓜V1引擎  |
| 17874219618  | 摸瓜V1引擎  |
| 14702406825  | 摸瓜V2引擎  |
| 16725171731  | 摸瓜V2引擎  |
| 15864168224  | 摸瓜V2引擎  |
| 13794778293  | 摸瓜V2引擎  |

## **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=, L=, O=Android, OU=Android, CN=JnK7eshBRqfxocAdvh0r%2FUIQuXQbOFtK0%2B0obBkFaXAO%2BxWFs61H4mWsHx41FvvwU0zJbtUGkAlOxvhuCfrwXQ%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2023-10-21 14:36:06+00:00 有效期至: 2123-09-27 14:36:06+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=JnK7eshBRqfxocAdvh0r%2FUIQuXQbOFtK0%2B0obBkFaXAO%2BxWFs61H4mWsHx41FvvwU0zJbtUGkAlOxvhuCfrwXQ%3D%3D 序列号: 0x17bd592 哈希算法: sha256 md5值: 088e6b2e1aa0c911f719cf74c1a189c1 sha1值: 8f46d051d1e345a89f860bd07669a39e83bfbccb sha256值: f521e0d5ad2f4790588d6c4f48e6318220ebab00fcb35481c7a6973f967fbfba sha512值: ba6e0bae69225988aa13fa89f0f5ac8468d5de696b6d70161c31b697e15e8362545dda7a183d710e5647cd9c794f17c4e79a65ad7c619e271a7f28de03c0241b 公钥算法: rsa 密钥长度: 2048 指纹: 762856b2ee78718579c035ca66efa400e44e20d41327b83629954c4c4fd75abf**

## **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.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.ACCESS\_MEDIA\_LOCATION | 危险 | 访问的任何地理位置 | 允许应用程序访问的任何地理位置持久保存在用户的共享集合 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE  | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| 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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.txcf.cronuss.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.txcf.cronuss.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.txcf.cronuss.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.txcf.cronuss.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.txcf.cronuss.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.txcf.cronuss.MainActivity | **Schemes**: guniuniu://, https://, **Hosts:** app.txcfgl.com,  |

**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。**