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

**思扬智动（ null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 | 思扬智动 |
| 版本 | null |
| 包名 | jshdbrgehej.nvsgehdhe.wihebdgr |
| 域名线索 | 69条 |
| URL线索 | 68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 | 6htry-SiYangzhd.apk |
| 文件大小 | 67.4MB |
| MD5值 | b25ae374a3a878f66de4bea90714c501 |
| SHA1值 | b37976f700fde5b09db3a1f6d6f50f9a7373e33f |
| SHA256值 | 8f50177b0a23297c80ed9e3874b49c86c240e33937e992d42d0faaf683c27f69 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 思扬智动 |
| 包名 | jshdbrgehej.nvsgehdhe.wihebdgr |
| 主活动Activity | im.cnzgsxeieu.ui.LaunchActivity |
| 安卓版本名称 | null |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| j.map.baidu.com | IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing  |
| api.ipify.org | IP: 104.26.13.205 所属国家: United States of America 地区: California 城市: San Francisco  |
| coub.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.aparat.com | IP: 185.147.178.11 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran  |
| ident.me | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| wapmap.baidu.com | IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing  |
| game.cailiao.im | 没有服务器地理信息.  |
| 2024.ipchaxun.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| myip.ipip.net | IP: 123.129.226.44 所属国家: China 地区: Shandong 城市: Jinan  |
| daup.map.baidu.com | IP: 110.242.74.236 所属国家: China 地区: Hebei 城市: Baoding  |
| d.alipay.com | IP: 111.202.5.209 所属国家: China 地区: Beijing 城市: Beijing  |
| 106.13.253.35 | IP: 106.13.253.35 所属国家: China 地区: Beijing 城市: Beijing  |
| m12345.com | IP: 75.2.19.62 所属国家: United States of America 地区: Washington 城市: Seattle  |
| live.cailiao.im | 没有服务器地理信息.  |
| d1nf62p0mer0p6.cloudfront.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| maps.google.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| d38ofppx0kewju.cloudfront.net | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| game.bjz.com | 没有服务器地理信息.  |
| ifconfig.me | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api.stripe.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| d2q5yxrukkeb7s.cloudfront.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.google.com | IP: 31.13.73.9 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| m.bjz.com | 没有服务器地理信息.  |
| youtube.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api.twitch.tv | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| client.map.baidu.com | IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing  |
| www.slf4j.org | IP: 195.15.222.169 所属国家: Switzerland 地区: Geneve 城市: Carouge  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| 192.200.1.242 | IP: 192.200.1.242 所属国家: United States of America 地区: New Jersey 城市: Jersey City  |
| 192.168.31.38 | IP: 192.168.31.38 所属国家: - 地区: - 城市: -  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |
| d1pu7q9g0ei114.cloudfront.net | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.smpte-ra.org | IP: 52.20.185.129 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| vop.baidu.com | IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| acs.m.taobao.com | IP: 203.119.204.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| openapi.baidu.com | IP: 110.242.69.36 所属国家: China 地区: Hebei 城市: Baoding  |
| youtube.googleapis.com | IP: 142.250.69.170 所属国家: United States of America 地区: California 城市: Mountain View  |
| ss3.4sqi.net | IP: 151.101.90.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| attheme.org | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| app.navi.baidu.com | IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing  |
| www.instagram.com | IP: 69.30.25.21 所属国家: United States of America 地区: Washington 城市: Seattle  |
| impyq.gz.bcebos.com | IP: 153.3.238.105 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| shibatch.sourceforge.net | IP: 104.18.13.149 所属国家: United States of America 地区: California 城市: San Francisco  |
| 106.13.253.90 | IP: 106.13.253.90 所属国家: China 地区: Beijing 城市: Beijing  |
| www.shareinstall.com.cn | 没有服务器地理信息.  |
| wealthextend.huanhuit.com | 没有服务器地理信息.  |
| api.gameshield.top | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| whois.pconline.com.cn | IP: 112.240.59.156 所属国家: China 地区: Shandong 城市: Zibo  |
| twitter.com | IP: 31.13.94.41 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| instagram.com | IP: 38.121.72.166 所属国家: United States of America 地区: Georgia 城市: Atlanta  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ntsc.ac.cn | IP: 159.226.242.43 所属国家: China 地区: Beijing 城市: Beijing  |
| daohang.map.baidu.com | IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| www.example.com | IP: 23.55.179.196 所属国家: Japan 地区: Osaka 城市: Ibaraki  |
| schemas.android.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.youtube.com | IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| m12345.cc | IP: 77.247.179.87 所属国家: Netherlands 地区: Noord-Brabant 城市: Roosendaal  |
| player.vimeo.com | IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |
| static-maps.yandex.ru | IP: 213.180.204.41 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| maps.googleapis | 没有服务器地理信息.  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| usher.ttvnw.net | IP: 13.35.202.83 所属国家: India 地区: Telangana 城市: Hyderabad  |
| 192.168.1.4 | IP: 192.168.1.4 所属国家: - 地区: - 城市: -  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| ip-api.com | IP: 208.95.112.1 所属国家: United States of America 地区: North Carolina 城市: Skyland  |
| stripe.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://map.baidu.com/zt/client/index/?fr=sdk\_[  | com/baidu/mapapi/utils/OpenClientUtil.java  |
| http://api.map.baidu.com/place/detail?uid=  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/place/search?  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/direction?  | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java  |
| http://app.navi.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://daohang.map.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://loc.map.baidu.com/cc.php  | com/baidu/location/b/d.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/f.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/g/k.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/g/k.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/g/k.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/g/k.java  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | com/baidu/location/indoor/a.java  |
| http://loc.map.baidu.com/check\_indoor\_data\_update  | com/baidu/location/indoor/mapversion/a/e.java  |
| https://loc.map.baidu.com/ios\_indoorloc  | com/baidu/location/indoor/mapversion/a/a.java  |
| http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/indoor/mapversion/c/a.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/c/e.java  |
| http://loc.map.baidu.com/gpsz  | com/baidu/location/c/a.java  |
| https://api.map.baidu.com/lbs\_sdkcc/report  | com/baidu/mapsdkplatform/comapi/b/a/c.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/custom/v2/getjsonstyle  | com/baidu/mapsdkplatform/comapi/map/h.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/custom/v2/getjsonstyle  | com/baidu/mapsdkplatform/comapi/map/h.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/a.java  |
| http://j.map.baidu.com/  | com/baidu/platform/domain/a.java  |
| http://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/a.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/b.java  |
| https://j.map.baidu.com/  | com/baidu/platform/domain/b.java  |
| https://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/b.java  |
| http://wapmap.baidu.com/s?tn=Detail&pid=  | com/baidu/platform/core/e/c.java  |
| http://map.baidu.com/?newmap=1&s=  | com/baidu/platform/core/e/e.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://192.200.1.242:1999/  | com/bjz/comm/net/UrlConstant.java  |
| http://m.bjz.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://106.13.253.35/  | com/bjz/comm/net/UrlConstant.java  |
| https://live.cailiao.im/  | com/bjz/comm/net/UrlConstant.java  |
| http://game.bjz.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://game.cailiao.im  | com/bjz/comm/net/UrlConstant.java  |
| http://192.168.1.4:20000/  | com/bjz/comm/net/UrlConstant.java  |
| https://106.13.253.90/  | com/bjz/comm/net/UrlConstant.java  |
| https://impyq.gz.bcebos.com/  | com/bjz/comm/net/UrlConstant.java  |
| http://ip-api.com/json/  | com/bjz/comm/net/UrlConstant.java  |
| https://wealthextend.huanhuit.com/  | com/bjz/comm/net/UrlConstant.java  |
| https://vop.baidu.com/  | com/bjz/comm/net/factory/ApiTranslateAudioFactory.java  |
| https://impyq.gz.bcebos.com/  | com/bjz/comm/net/utils/HttpUtils.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/HttpUrlSource.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/Pinger.java  |
| http://%s:%d/%s  | com/danikula/videocache/HttpProxyCacheServer.java  |
| https://2024.ipchaxun.com  | com/app/protect/AppProtectManager.java  |
| https://myip.ipip.net  | com/app/protect/AppProtectManager.java  |
| https://ifconfig.me  | com/app/protect/AppProtectManager.java  |
| https://ident.me  | com/app/protect/AppProtectManager.java  |
| https://api.ipify.org  | com/app/protect/AppProtectManager.java  |
| https://whois.pconline.com.cn/ipJson.jsp?ip=&json=true  | com/app/protect/AppProtectManager.java  |
| https://api.gameshield.top/log\_error.php  | com/app/protect/AppProtectManager.java  |
| https://acs.m.taobao.com/gw/mtop.common.getTimestamp/  | com/app/protect/AppProtectManager.java  |
| http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt  | com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java  |
| https://stripe.com/docs/stripe.js.  | com/stripe/android/Stripe.java  |
| https://stripe.com/docs/stripe.js  | com/stripe/android/Stripe.java  |
| https://api.stripe.com  | com/stripe/android/net/StripeApiHandler.java  |
| https://stripe.com/api  | com/stripe/android/net/StripeApiHandler.java  |
| https://twitter.com/stripestatus,  | com/stripe/android/net/StripeApiHandler.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SlidingScaleTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/tablayout/SlidingTabLayout.java  |
| http://xml.apache.org/xslt  | com/socks/library/klog/XmlLog.java  |
| https://static-maps.yandex.ru/1.x/?ll=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&pt=%.6f,%.6f,vkbkm&lang=%s  | im/cnzgsxeieu/messenger/AndroidUtilities.java  |
| https://static-maps.yandex.ru/1.x/?ll=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&lang=%s  | im/cnzgsxeieu/messenger/AndroidUtilities.java  |
| http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s&center=%.6f,%.6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll&copyright=1&dpiType=ph&markers=%.6f,%.6f&markerStyles=l,,red  | im/cnzgsxeieu/messenger/AndroidUtilities.java  |
| http://api.map.baidu.com/staticimage/v2?ak=%s&mcode=%s&center=%.6f,%.6f&width=%d&height=%d&zoom=%d&scale=%d&coordtype=gcj02ll&copyright=1&dpiType=ph  | im/cnzgsxeieu/messenger/AndroidUtilities.java  |
| https://instagram.com/  | im/cnzgsxeieu/messenger/MessageObject.java  |
| https://www.instagram.com/explore/tags/  | im/cnzgsxeieu/messenger/MessageObject.java  |
| https://twitter.com/  | im/cnzgsxeieu/messenger/MessageObject.java  |
| https://twitter.com/hashtag/  | im/cnzgsxeieu/messenger/MessageObject.java  |
| https://static-maps  | im/cnzgsxeieu/messenger/ImageLoader.java  |
| https://maps.googleapis  | im/cnzgsxeieu/messenger/ImageLoader.java  |
| https://m12345.com/dl  | im/cnzgsxeieu/messenger/ContactsController.java  |
| https://m12345.cc/install.html?appkey=aa717156fa6e34325d3d4a7004a6647a  | im/cnzgsxeieu/messenger/MessagesController.java  |
| http://www.shareinstall.com.cn/js-test.html?appkey=aa717156fa6e34325d3d4a7004a6647a  | im/cnzgsxeieu/messenger/MessagesController.java  |
| https://www.youtube.com/embed/  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://youtube.googleapis.com/v/  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://www.youtube.com/get\_video\_info?  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://www.youtube.com  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://player.vimeo.com/video/%s/config  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://api.twitch.tv/kraken/streams/%s?stream\_type=all  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://api.twitch.tv/api/channels/%s/access\_token  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| https://coub.com/api/v2/coubs/%s.json  | im/cnzgsxeieu/messenger/utils/PlayerUtils.java  |
| http://www.example.com  | im/cnzgsxeieu/messenger/support/customtabsclient/shared/CustomTabsHelper.java  |
| http://www.google.com  | im/cnzgsxeieu/messenger/browser/Browser.java  |
| https://www.google.com/resolve?name=  | im/cnzgsxeieu/tgnet/ConnectionsManager.java  |
| https://d1pu7q9g0ei114.cloudfront.net/dns-query  | im/cnzgsxeieu/tgnet/NetworkConfig.java  |
| https://d2q5yxrukkeb7s.cloudfront.net/dns-query  | im/cnzgsxeieu/tgnet/NetworkConfig.java  |
| https://m12345.com/deactivate?phone=  | im/cnzgsxeieu/ui/TwoStepVerificationActivity.java  |
| https://m12345.cc/deactivate?phone=  | im/cnzgsxeieu/ui/TwoStepVerificationActivity2.java  |
| http://maps.google.com/maps?saddr=%f,%f&daddr=%f,%f  | im/cnzgsxeieu/ui/LocationActivity.java  |
| http://youtube.com  | im/cnzgsxeieu/ui/ArticleViewer.java  |
| https://m12345.com/embed  | im/cnzgsxeieu/ui/ArticleViewer.java  |
| https://m12345.com/deactivate?phone=  | im/cnzgsxeieu/ui/PassportActivity.java  |
| https://m12345.com/proxy?  | im/cnzgsxeieu/ui/ProxySettingsActivity.java  |
| https://m12345.com/socks?  | im/cnzgsxeieu/ui/ProxySettingsActivity.java  |
| https://m12345.com  | im/cnzgsxeieu/ui/ChatActivity.java  |
| http://m12345.com  | im/cnzgsxeieu/ui/ChatActivity.java  |
| https://m12345.com/authtoken/  | im/cnzgsxeieu/ui/ChatActivity.java  |
| https://openapi.baidu.com/oauth/2.0/token  | im/cnzgsxeieu/ui/ChatActivity.java  |
| https://vop.baidu.com/pro\_api  | im/cnzgsxeieu/ui/ChatActivity.java  |
| https://www.youtube.com/iframe\_api\  | im/cnzgsxeieu/ui/components/EmbedBottomSheet.java  |
| http://youtube.com  | im/cnzgsxeieu/ui/components/EmbedBottomSheet.java  |
| https://www.youtube.com  | im/cnzgsxeieu/ui/components/EmbedBottomSheet.java  |
| https://m12345.com/  | im/cnzgsxeieu/ui/components/URLSpanNoUnderline.java  |
| https://www.youtube.com/embed/  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://youtube.googleapis.com/v/  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://www.youtube.com/get\_video\_info?  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://www.youtube.com  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://player.vimeo.com/video/%s/config  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://api.twitch.tv/kraken/streams/%s?stream\_type=all  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://api.twitch.tv/api/channels/%s/access\_token  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://coub.com/api/v2/coubs/%s.json  | im/cnzgsxeieu/ui/components/WebPlayerView.java  |
| https://192.168.31.38:8080/v1/token  | im/cnzgsxeieu/ui/hui/visualcall/AliRtcConstants.java  |
| https://m12345.com  | im/cnzgsxeieu/ui/hui/discovery/QrScanActivity.java  |
| http://m12345.com  | im/cnzgsxeieu/ui/hui/discovery/QrScanActivity.java  |
| https://m12345.com/authtoken/  | im/cnzgsxeieu/ui/hui/discovery/QrScanActivity.java  |
| http://shibatch.sourceforge.net/\n\n  | im/cnzgsxeieu/ui/utils/translate/ssrc/SSRC.java  |
| http://www.ntsc.ac.cn  | im/cnzgsxeieu/ui/utils/timer/OrderCountDownHelper.java  |
| https://d.alipay.com  | im/cnzgsxeieu/ui/wallet/WalletRechargeH5Activity.java  |
| https://attheme.org?slug=  | im/cnzgsxeieu/ui/actionbar/Theme.java  |
| https://ss3.4sqi.net/img/categories\_v2/  | im/cnzgsxeieu/ui/adapters/BaseLocationAdapter.java  |
| https://d38ofppx0kewju.cloudfront.net/dns-query  | im/cnzgsxeieu/network/NetworkConstant.java  |
| https://d1nf62p0mer0p6.cloudfront.net/dns-query  | im/cnzgsxeieu/network/NetworkConstant.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/MDC.java  |
| http://www.slf4j.org/codes.html  | org/slf4j/LoggerFactory.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com  | com/danikula/videocache/HttpUrlSource.java  |
| support@stripe.com  | com/stripe/android/net/StripeApiHandler.java  |
| sms@stel.com  | im/cnzgsxeieu/ui/ChangePhoneActivity.java  |
| login@stel.com sms@stel.com  | im/cnzgsxeieu/ui/LoginActivity.java  |
| sms@stel.com  | im/cnzgsxeieu/ui/PassportActivity.java  |
| sms@stel.com  | im/cnzgsxeieu/ui/CancelAccountDeletionActivity.java  |
| login@stel.com sms@stel.com  | im/cnzgsxeieu/ui/hui/login/HloginActivity.java  |
| login@stel.com  | im/cnzgsxeieu/ui/hui/login/LoginContronllerBaseActivity.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118  | com/baidu/mapsdkplatform/comapi/util/b.java  |
| 14058229493  | im/cnzgsxeieu/messenger/Utilities.java  |

## **5. 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=rtpqheqrogllkry, ST=szftmflhapeoqoy, L=kyeqaspfkukswva, O=zyl1748917602817, OU=zai1748917602817, CN=Xnzv1748917602817 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-03 02:26:42+00:00 有效期至: 2075-05-22 02:26:42+00:00 发行人: C=rtpqheqrogllkry, ST=szftmflhapeoqoy, L=kyeqaspfkukswva, O=zyl1748917602817, OU=zai1748917602817, CN=Xnzv1748917602817 序列号: 0x2d11ccb5 哈希算法: sha1 md5值: 136624eca546de64af25a802f8e41d02 sha1值: dbe66ad5025bbdae9aafb884f713d8893c932a3e sha256值: 08c956eca2080acc33cd39f1b6c1665080730fef3b5a059c38052d5782f89a4c sha512值: a760995525844e1bf53fbd67acd358412209176c5cbd984e12601c85c51a5306a48c89cd59e49af5279fb7e1bbe2f81e19743b2207bfccd42fb6a5b9b7c7a6ba 公钥算法: rsa 密钥长度: 1024 指纹: a5b37fd2da0dc74966ec05f64ff13aaff4256c11a49204a1d6937fa3b5413518**

## **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。**