MoGua

抖音18+ 1.3.4.APK 分析报告

APP名称: 抖音18+

包名:	com.smd.douyin18.app
域名线索:	64条
URL线索:	89条
邮箱线索:	2条
分析日期:	2025年5月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 抖音18 .apk
文件大小: 25.55MB
MD5值: 100130f6fd3ce5e6684a7e8280cdcae8
SHA1值: 736cfbdbb10b2784b31c688c31c1c809bac2f87e
SHA256值: 5456f28b43bc466cea2750dee3901a470a3db77cc87c43a33a52bfe83c5e1748

APP 信息

App名称: 抖音18+
包名: com.smd.douyin18.app
主活动Activity: com.osea.app.WelcomeActivity
安卓版本名称: 1.3.4
安卓版本: 134

域名线索

域名	服务器信息
graph.zalo.me	**IP**: 49.213.114.145 **所属国家**: Viet Nam **地区**: Ho Chi Minh **城市**: Ho Chi Minh City **纬度**: 10.750000 **经度**: 106.666672
www.mob.com	**IP**: 116.62.130.46 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
pslog.umeng.com	**IP**: 59.82.31.160 **所属国家**: China **地区**: Beijing

	城市: Beijing **纬度**: 39.907501 **经度**: 116.397232
schemas.android.com	没有服务器地理信息.
pre-c.umsns.com	**IP**: 59.82.17.247 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
alogus.umeng.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
s3.amazonaws.com	**IP**: 52.216.111.13 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.043720 **经度**: -77.487488
at.umeng.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423

openapi.zaloapp.com	**IP**: 103.252.115.53 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
ai.login.umeng.com	**IP**: 59.82.112.112 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
ulogs.umengcloud.com	**IP**: 223.109.148.179 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.example.com	**IP**: 93.184.216.34 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.043720 **经度**: -77.487488
mobile.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
cfg.flurry.com	**IP**: 98.136.147.20 **所属国家**: United States of America **地区**: New York **城市**: New York City

	纬度: 40.731323 **经度**: -73.990089
github.com	IP: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
www.youtube.com	IP: 104.244.46.185 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
developer.umeng.com	IP: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
play.google.com	IP: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 49.7.37.118 **所属国家**: China

open.weibo.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
s3-us-west-1.amazonaws.com	**IP**: 52.219.121.112 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
oauth.zaloapp.com	**IP**: 199.59.148.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
www.yahoo.com	**IP**: 180.222.102.201 **所属国家**: Taiwan (Province of China) **地区**: Taipei **城市**: Taipei **纬度**: 25.047760 **经度**: 121.531853
graph.qq.com	**IP**: 175.27.9.43 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
m.youtube.com	**IP**: 104.244.46.186 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446

alogsus.umeng.com	**IP**: 223.109.148.130 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
hb.yunti123.com	**IP**: 79.137.198.229 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752220 **经度**: 37.615559
www.openssl.org	**IP**: 23.34.36.190 **所属国家**: Japan **地区**: Osaka **城市**: Osaka **纬度**: 34.693890 **经度**: 135.502213
sfo2.digitaloceanspaces.com	**IP**: 138.68.32.225 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
dev.rubaoo.com	**IP**: 121.43.108.235 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
	IP: 218.91.197.67 **所属国家**: China **地区**: Jiangsu

aaid.umeng.com	**城市**: Nantong **纬度**: 32.030281 **经度**: 120.874718
www.googleapis.com	**IP**: 172.217.163.42 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
data.flurry.com	**IP**: 69.147.80.15 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
cdn.flurry.com	**IP**: 69.147.80.15 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
s.nqwn3.xyz	**IP**: 68.183.248.69 **所属国家**: United States of America **地区**: California **城市**: Santa Clara **纬度**: 37.354111 **经度**: -121.955238
log.umsns.com	**IP**: 59.82.31.154 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232

xmlpull.org	**IP**: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
service.cmp.oath.com	**IP**: 152.195.57.116 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.034081 **经度**: -77.488503
ams3.digitaloceanspaces.com	**IP**: 5.101.110.225 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.374031 **经度**: 4.889690
openmobile.qq.com	**IP**: 175.27.9.43 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ns.adobe.com	没有服务器地理信息.
sgp1.digitaloceanspaces.com	**IP**: 103.253.144.208 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
	IP: 218.30.115.40

service.weibo.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.umeng.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
api.weibo.com	**IP**: 49.7.37.118 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
issuetracker.google.com	**IP**: 172.217.163.46 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dl.gzmad.xyz	没有服务器地理信息.
api.5nxam.xyz	**IP**: 157.230.199.123 **所属国家**: United States of America **地区**: California **城市**: Santa Clara **纬度**: 37.354111 **经度**: -121.955238
	IP: 74.6.160.138 **所属国家**: United States of America **地区**: New York

api.login.yahoo.com	**城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
nyc3.digitaloceanspaces.com	**IP**: 162.243.189.2 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.719936 **经度**: -74.005013
acs.amazonaws.com	没有服务器地理信息.
adlog.flurry.com	**IP**: 74.6.160.107 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
ads.flurry.com	**IP**: 74.6.160.107 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
api.yunti123.com	**IP**: 79.137.198.229 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752220 **经度**: 37.615559
c.umsns.com	**IP**: 59.82.60.44 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650

	经度: 120.161423
accounts.google.com	**IP**: 172.217.163.45 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
dev.centralize.zaloapp.com	**IP**: 23.101.24.70 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
www.ngs.ac.uk	**IP**: 130.246.140.235 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: Appleton **纬度**: 51.709511 **经度**: -1.361360
ulogs.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.weixin.qq.com	**IP**: 109.244.145.152 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 31.13.90.33 **所属国家**: United States of America **地区**: Texas

centralized.zaloapp.com	**城市**: Fort Worth **纬度**: 32.725410 **经度**: -97.320847
plbslog.umeng.com	**IP**: 36.156.202.78 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
..m3u8	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://dev.rubaoo.com/TimeDiaryV2/s/MmU5bHA=	com/hanbing/wltc/han.java
http://openapi.zaloapp.com/query	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://graph.zalo.me/v2.0/me	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://oauth.zaloapp.com/v3/mobile/access_token	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://graph.zalo.me/v2.0/oa/message	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://graph.zalo.me/v2.0/apprequests	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://graph.zalo.me/v2.0/me/feed	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://graph.zalo.me/v2.0/me/message	com/zing/zalo/zalosdk/oauth/OpenAPIService.java
https://play.google.com/store/apps/details?id=	com/zing/zalo/zalosdk/core/helper/AppInfo.java
https://centralized.zaloapp.com	com/zing/zalo/devicetrackingsdk/Constant.java
https://centralized.zaloapp.com/zaid/mobile/android	com/zing/zalo/devicetrackingsdk/BaseAppInfo.java
https://centralized.zaloapp.com/sdk/mobile/android	com/zing/zalo/devicetrackingsdk/BaseAppInfo.java
https://centralized.zaloapp.com/id/mobile/android	com/zing/zalo/devicetrackingsdk/BaseAppInfo.java
http://dev.centralize.zaloapp.com/appsv2/mobile/version	com/zing/zalo/devicetrackingsdk/BaseAppInfo.java
https://centralized.zaloapp.com/oauth/mobile/android	com/zing/zalo/devicetrackingsdk/BaseAppInfo.java
https://centralized.zaloapp.com/apps/mobile/android	com/zing/zalo/devicetrackingsdk/a.java

http://dev.centralize.zaloapp.com/appsv2/mobile/android	com/zing/zalo/devicetrackingsdk/a.java
http://dev.centralize.zaloapp.com	com/zing/zalo/devicetrackingsdk/a.java
https://centralized.zaloapp.com/apps/mobile/android	com/zing/zalo/devicetrackingsdk/AppTracker.java
http://dev.centralize.zaloapp.com/appsv2/mobile/android	com/zing/zalo/devicetrackingsdk/AppTracker.java
https://centralized.zaloapp.com/apps/mobile/explore/android	com/zing/zalo/devicetrackingsdk/AppTracker.java
http://dev.centralize.zaloapp.com/appsv2/mobile/explore/android	com/zing/zalo/devicetrackingsdk/AppTracker.java
http://schemas.android.com/apk/res/android	com/commonview/view/view/ProgressBarCircular.java
http://[0-9a-zA-Z	com/osea/utils/utils/StringUtils.java
https://)(.+)(\\.m3u8)(($)	com/osea/utils/utils/StringUtils.java
http://api.yunti123.com/%s	com/osea/player/model/musical/MusicHelperImpl.java
https://www.youtube.com/watch	com/osea/player/webview/PvWebViewThirdLinkActivity.java
https://m.youtube.com/watch	com/osea/player/webview/PvWebViewThirdLinkActivity.java
http://api.5nxam.xyz	com/osea/commonbusiness/BuildConfig.java
http://api.5nxam.xyz	com/osea/commonbusiness/engineermode/EngineerCache.java
http://s.nqwn3.xyz/static/images/share/logo.png	com/osea/commonbusiness/reward/ShareRewardImpl.java
https://api.weibo.com/2/friendships/friends.json	com/osea/commonbusiness/api/ApiOthers.java
http://api2.	com/osea/commonbusiness/api/DynamicBackupDomainManager.java

http://api.	com/osea/commonbusiness/api/DynamicBackupDomainManager.java
https://hb.yunti123.com	com/osea/commonbusiness/api/osea/ApiClientCreator.java
http://api.5nxam.xyz	com/osea/commonbusiness/api/osea/ApiClientCreator.java
http://hb.yunti123.com/share/invite?userId=	com/osea/commonbusiness/api/osea/ApiClientCreator.java
http://api.5nxam.xyz	com/osea/commonbusiness/api/osea/DNSManger.java
http://api.5nxam.xyz;	com/osea/commonbusiness/api/osea/DNSManger.java
http://api.yunti123.com/task/center.html	com/osea/commonbusiness/model/v1/HpConfig.java
http://api.5nxam.xyz	com/osea/app/BuildConfig.java
http://api.5nxam.xyz	com/osea/app/ApplicationInit.java
http://s.nqwn3.xyz/looba/gold/index.html	com/osea/app/ui/UserHomeFragmentV1.java
http://s.nqwn3.xyz/looba/friend.html	com/osea/app/ui/UserHomeFragmentV1.java
http://s.nqwn3.xyz/looba/invite.html	com/osea/app/ui/UserHomeFragmentV1.java
https://accounts.google.com/o/oauth2/auth	com/osea/social/base/Utils.java
https://www.googleapis.com/oauth2/v4/token	com/osea/social/base/Utils.java
https://www.googleapis.com/plus/v1/people/	com/osea/social/base/Utils.java
https://ams3.digitaloceanspaces.com	com/osea/upload/upload/UploadTaskManagerImpl.java
https://nyc3.digitaloceanspaces.com	com/osea/upload/upload/UploadTaskManagerImpl.java
https://sfo2.digitaloceanspaces.com	com/osea/upload/upload/UploadTaskManagerImpl.java

https://sgp1.digitaloceanspaces.com	com/osea/upload/upload/UploadTaskManagerImpl.java
http://s.nqwn3.xyz/gold/help.html	com/osea/me/share/CommonShareDialog.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/ObservableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/SingleLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/CompletableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/MaybeLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/FlowableLife.java
https://data.flurry.com/v1/flr.do	com/flurry/sdk/bs.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cm.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/bz.java
http://www.example.com	com/flurry/sdk/ee.java
https://data.flurry.com/aap.do	com/flurry/sdk/br.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/eg.java
https://service.cmp.oath.com/cmp/v0/location/eu	com/flurry/sdk/ads/bd.java
https://adlog.flurry.com	com/flurry/sdk/ads/fx.java
http://adlog.flurry.com	com/flurry/sdk/ads/fx.java
https://cdn.flurry.com/vast/videocontrols/v2/android.zip	com/flurry/sdk/ads/s.java

https://issuetracker.google.com/issues/68454482	com/flurry/sdk/ads/gb.java
https://play.google.com/store/apps/details?id=	com/flurry/sdk/ads/o.java
https://ads.flurry.com/v19/getAds.do	com/flurry/sdk/ads/q.java
http://ads.flurry.com/v19/getAds.do	com/flurry/sdk/ads/q.java
http://cdn.flurry.com/adSpaceStyles.dev/images/bttn-close-bw.png\	com/flurry/sdk/ads/iw.java
http://xmlpull.org/v1/doc/features.html	com/flurry/sdk/ads/gs.java
http://www.example.com	com/flurry/sdk/ads/dj.java
https://cdn.flurry.com/sdkAssets/bttn-close-bw.png\	com/flurry/sdk/ads/ir.java
http://www.yahoo.com	com/flurry/sdk/ads/iu.java
https://play.google.com/store/apps/details?id=	com/flurry/sdk/ads/gk.java
https://s3-us-west-1.amazonaws.com	com/amazonaws/services/s3/AmazonS3Client.java
http://acs.amazonaws.com/groups/global/AllUsers	com/amazonaws/services/s3/model/GroupGrantee.java
http://acs.amazonaws.com/groups/global/AuthenticatedUsers	com/amazonaws/services/s3/model/GroupGrantee.java
http://acs.amazonaws.com/groups/s3/LogDelivery	com/amazonaws/services/s3/model/GroupGrantee.java
http://www.w3.org/2001/XMLSchema-instance	com/amazonaws/services/s3/model/transform/AclXmlFactory.java
http://s3.amazonaws.com/doc/2006-03-01/	com/amazonaws/services/s3/internal/Constants.java
http://www.ngs.ac.uk/tools/jcepolicyfiles	com/amazonaws/services/s3/internal/crypto/EncryptionUtils.java
http://log.umsns.com/link/qq/download/	com/umeng/qq/handler/UmengQZoneHandler.java

https://graph.qq.com/oauth2.0/me?access_token=	com/umeng/qq/handler/j.java
https://graph.qq.com/oauth2.0/me?access_token=	com/umeng/qq/handler/UmengQQHandler.java
http://log.umsns.com/link/qq/download/	com/umeng/qq/handler/UmengQQHandler.java
https://openmobile.qq.com/user/get_simple_userinfo?status_os=	com/umeng/qq/handler/UmengQQHandler.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	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://open.weibo.cn/oauth2/authorize?	com/umeng/socialize/handler/SinaSimplyHandler.java

https://at.umeng.com/9XX5ry?cid=476	com/umeng/socialize/handler/SinaSimplyHandler.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/socialize/utils/UrlUtil.java
https://log.umsns.com/	com/umeng/socialize/view/OauthDialog.java
http://service.weibo.com/share/mobilesdk.php	com/umeng/socialize/sina/params/ShareRequestParam.java
http://service.weibo.com/share/mobilesdk_uppic.php	com/umeng/socialize/sina/params/ShareRequestParam.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://api.weibo.com/2/users/show.json	com/umeng/socialize/net/h.java
https://api.weibo.com/oauth2/getaid.json	com/umeng/socialize/net/a.java
https://mobile.umeng.com/images/pic/home/social/img-1.png	com/umeng/socialize/net/LinkcardRequest.java
https://api.weibo.com/oauth2/revokeoauth2	com/umeng/socialize/net/c.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/i.java

https://api.weixin.qq.com/sns/userinfo?access_token=	com/umeng/weixin/handler/UmengWXHandler.java
https://api.weixin.qq.com/sns/oauth2/access_token?	com/umeng/weixin/handler/UmengWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?	com/umeng/weixin/handler/UmengWXHandler.java
https://at.umeng.com/f8HHDi?cid=476	com/umeng/weixin/handler/UmengWXHandler.java
http://log.umsns.com/link/weixin/download/	com/umeng/weixin/handler/UmengWXHandler.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=	com/umeng/weixin/handler/UmengWXHandler.java
http://www.mob.com	Mogua Engine V1
http://dl.gzmad.xyz/Osea.apk	Mogua Engine V1
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libimagepipeline.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

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

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java
19871128593	lib/armeabi-v7a/libve.so
19880600936	lib/armeabi-v7a/libve.so
19871528595	lib/armeabi-v7a/libve.so
19880900949	lib/armeabi-v7a/libve.so
19871528599	lib/armeabi-v7a/libve.so
19890601201	lib/armeabi-v7a/libve.so
19681420127	lib/armeabi-v7a/libve.so
19861028591	lib/armeabi-v7a/libve.so
19911351932	lib/armeabi-v7a/libve.so

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

🔑 硬编码敏感信息

可能的敏感信息
"account_auth_provide" : "com.llaboo.app.provider"
"account_auth_type" : "com.llaboo.app"
"account_manage_authorize_failed" : "Authorization failed"
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"flurry_app_key" : "FKKRQQJQGWP7WFJS9B5B"
"google_api_key" : "AIzaSyAacemaQscYnXKlTAABacB1oBWNzD49UvQ"
"google_crash_reporting_api_key" : "AIzaSyAacemaQscYnXKlTAABacB1oBWNzD49UvQ"
"kakao_app_key" : "osea-replace-it"
"kakao_client_secret" : "osea-replace-it"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"

"ssdk_cmcc_login_one_key" : "单机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"tip_cannot_find_user" : "Cannot find related user"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og indtast koden, som er vist ovenfor."
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"com_facebook_device_auth_instructions" : "facebook.com/device 'ਤੇ ਵਿਜ਼ਿਟ ਕਰੋ ਅਤੇ ਉੱਪਰ ਦਿੱਤੇ ਕੋਡ ਨੂੰ ਦਾਖ਼ਲ ਕਰੋ।"
"com_facebook_device_auth_instructions" : "facebook.com/device ஐப் பார்வையிட்டு, மேலே காட்டப்பட்ட குறியீட்டை உள்ளிடவும்."
"com_facebook_device_auth_instructions" : "Gå til facebook.com/device og skriv inn koden som vises over."
"com_facebook_device_auth_instructions" : "Gehe zu facebook.com/device und gib den oben angezeigten Code ein."
"com_facebook_device_auth_instructions" : "facebook.com/deviceని సందర్శించి ఎగువన చూపిన కోడ్‌ను నమోదు చేయండి."
"com_facebook_device_auth_instructions" : "Besoek facebook.com/device en voer die kode wat hierbo gewys word, in."
"com_facebook_device_auth_instructions" : "ไปที่ facebook.com/device แล้วป้อนรหัสที่ปรากฏด้านล่าง"

"com_facebook_device_auth_instructions" : "Siirry osoitteeseen facebook.com/device ja anna oheinen koodi."
"com_facebook_device_auth_instructions" : "facebook.com/device पर विज़िट करें और ऊपर दिखाया गया कोड डालें."
"com_facebook_device_auth_instructions" : "Truy cập facebook.com/device và nhập mã được hiển thị bên trên."
"com_facebook_device_auth_instructions" : "Navštívte stránku facebook.com/device a zadajte kód zobrazený vyššie."
"com_facebook_device_auth_instructions" : "Πηγαίνετε στη διεύθυνση facebook.com/device και εισαγάγετε τον παραπάνω κωδικό."
"com_facebook_device_auth_instructions" : "facebook.com/device സന്ദർശിച്ച് മുകളിൽ കാണിച്ചിരിക്കുന്ന കോഡ് നൽകുക."
"com_facebook_device_auth_instructions" : "Ga naar facebook.com/device en voer de bovenstaande code in."
"com_facebook_device_auth_instructions" : "Odwiedź stronę facebook.com/device i wprowadź powyższy kod."
"com_facebook_device_auth_instructions" : "Puntahan ang facebook.com/device at ilagay ang code na ipinapakita sa itaas."
"com_facebook_device_auth_instructions" : "facebook.com/device দেখুন এবং উপরে দেখানো কোডটিকে প্রবেশ করান।"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di bawah ini."
"com_facebook_device_auth_instructions" : "facebook.com/device ಗೆ ಭೇಟಿ ನೀಡಿ ಮತ್ತು ಮೇಲೆ ತೋರಿಸಿದ ಕೋಡ್ ಅನ್ನು ನಮೂದಿಸಿ."
"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."
"com_facebook_device_auth_instructions" : "تفضل بزيارة facebook.com/device وإدخال الرمز الموضح أعلاه."
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "Posjetitw facebook.com/device i unesite gore prikazani kôd."
"com_facebook_device_auth_instructions" : "facebook.com/device भेट द्या आणि वरील कोड प्रविष्ट करा."
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."

"com_facebook_device_auth_instructions" : "Přejděte na facebook.com/device a zadejte nahoře uvedený kód."
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"com_facebook_device_auth_instructions" : "Lawati facebook.com/device dan masukkan kod yang ditunjukkan di atas."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e inserisci il codice mostrato qui sotto."
"com_facebook_device_auth_instructions" : "facebook.com/device</b&gt ની મુલકાત લો; અને ઉપર આપેલો કોડ દાખલ કરો."
"com_facebook_device_auth_instructions" : "Keresd fel a facebook.com/device címet, és írd be a fent megjelenített kódot."
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"com_facebook_device_auth_instructions" : "Gå till facebook.com/device och skriv in koden som visas ovan."
"com_facebook_device_auth_instructions" : "יש לבקר בכתובת facebook.com/device</b&gt ולהזין את הקוד המוצג למעלה"
"com_facebook_device_auth_instructions" : "Accédez à facebook.com/device et entrez le code affiché ci-dessus."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e insere o código apresentado abaixo."
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"com_facebook_device_auth_instructions" : "Kunjungi facebook.com/device dan masukkan kode yang ditampilkan di atas."
"com_facebook_device_auth_instructions" : "Acesse facebook.com/device e insira o código mostrado acima."
"com_facebook_device_auth_instructions" : "Visita facebook.com/device e introduce el código que se muestra más arriba."

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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
com.smd.douyin18.app.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.RECEIVE_USER_PRESENT	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.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_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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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_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

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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.AUTHENTICATE_ACCOUNTS	危险	充当帐户验证器	允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码
android.permission.WRITE_SYNC_SETTINGS	正常	写入同步设置	允许应用程序修改同步设置,例如是否为联系人启用同步
android.permission.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference

com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.osea.app.WelcomeActivity	Schemes: douyin18://, Hosts: web,
com.osea.videoedit.ui.VideoEditorActivity	Schemes: video_edit://, Hosts: com.osea.videoedit,
com.facebook.CustomTabActivity	Schemes: @string/fb_login_protocol_scheme://,