MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

广告拦截器 1.0.4.APK

APP名称:	广告拦截器

包名:	com.anguomob.adblock
域名线索:	40条
URL线索:	49条
邮箱线索:	1条
分析日期:	2022年1月18日 23:08

文件信息

文件名: 22f998904d8d79072e8c62a96e2664c7.apk
文件大小: 28.56MB
MD5值: 22f998904d8d79072e8c62a96e2664c7
SHA1值: 71ae31e9eca26aae7590b80a0597d4afd5288350
SHA256值: 63bc215861ee874300a01990228bd45f8f22adb30bb9c281b7c2c5d006f9a007

APP 信息

App名称: 广告拦截器
包名: com.anguomob.adblock
主活动Activity: ui.SplashActivity
安卓版本名称: 1.0.4

安卓版本: 5

域名线索

域名	是否危险域名	服务器信息
astat.bugly.cros.wr.pvp.net	good	**IP:** 170.106.135.32 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.774929 经度: -122.419418 查看地图: Google Map
debugtbs.qq.com	good	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
pms.mb.qq.com	good	**IP:** 121.51.158.70 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
i.snssdk.com	good	**IP:** 140.249.226.225 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map

域名	是否危险域名	服务器信息
www.qq.com	good	**IP:** 175.27.8.138 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
soft.tbs.imtt.qq.com	good	**IP:** 182.254.59.187 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
pslog.umeng.com	good	**IP:** 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul 纬度: 37.568260 经度: 126.977829 查看地图: Google Map
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
app.blokada.org	good	**IP:** 142.251.43.19 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map
alogus.umeng.com	good	**IP:** 59.82.29.246 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
www.chengzijianzhan.com	good	**IP:** 119.96.66.250 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
apps.oceanengine.com	good	**IP:** 111.160.44.230 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
mdc.html5.qq.com	good	**IP:** 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
plbslog.umeng.com	good	**IP:** 59.82.66.230 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
mon.snssdk.com	good	**IP:** 182.254.59.213 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
alogsus.umeng.com	good	**IP:** 106.11.43.144 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
plugin-patch-api.bytedance.com	good	**IP:** 125.39.216.239 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
android.bugly.qq.com	good	**IP:** 109.244.244.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
phishing.army	good	**IP:** 104.21.65.39 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
developer.umeng.com	good	**IP:** 59.82.31.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
www.samsungapps.com	good	**IP:** 54.229.93.185 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.343990 经度: -6.267190 查看地图: Google Map
ulogs.umeng.com	good	**IP:** 106.11.86.69 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
aaid.umeng.com	good	**IP:** 106.8.130.61 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map
energized.pro	good	**IP:** 172.67.221.49 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map
www.yzdzy.com	good	**IP:** 49.232.2.131 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
go.blokada.org	good	**IP:** 172.217.163.51 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map
log.tbs.qq.com	good	**IP:** 109.244.244.37 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
tbsrecovery.imtt.qq.com	good	**IP:** 109.244.244.237 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
debugx5.qq.com	good	**IP:** 175.27.9.46 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
blokada.org	good	**IP:** 172.67.167.56 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
ouplog.umeng.com	good	**IP:** 47.74.172.6 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
api.blocka.net	good	**IP:** 216.239.34.21 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.toutiaopage.com	good	**IP:** 125.39.216.242 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
play.google.com	good	**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 查看地图: Google Map
www.slf4j.org	good	**IP:** 83.166.144.67 所属国家: Switzerland 地区: Geneve 城市: Carouge 纬度: 46.180962 经度: 6.139210 查看地图: Google Map
ulogs.umengcloud.com	good	**IP:** 106.11.40.44 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
github.com	good	**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 查看地图: Google Map

域名	是否危险域名	服务器信息
sf6-ttcdn-tos.pstatp.com	good	**IP:** 42.81.54.252 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://mon.snssdk.com/monitor/appmonitor/v2/settings	com/bytedance/pangle/helper/d.java
https://mon.snssdk.com/monitor/collect/	com/bytedance/pangle/helper/d.java
https://plugin-patch-api.bytedance.com/api/plugin/config/v2/	com/bytedance/pangle/download/e.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/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://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.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

URL信息	Url所在文件
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/i.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
www.qq.com	com/tencent/smtt/sdk/m.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/m.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java

URL信息	Url所在文件
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/n.java
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://www.yzdzy.com/appshare.php?id=	com/anguomob/total/utils/SettingUtils.java
http://play.google.com/store/apps/details?id=	com/anguomob/total/utils/SettingUtils.java
https://www.yzdzy.com/app/ad/v3/update.php	com/anguomob/total/common/ApiConstant.java
https://www.yzdzy.com	com/anguomob/total/common/ApiConstant.java
www.chengzijianzhan.com	com/ss/android/downloadlib/addownload/compliance/b.java
www.toutiaopage.com/tetris/page	com/ss/android/downloadlib/addownload/compliance/b.java
https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/downloadlib/addownload/compliance/b.java
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/downloadlib/addownload/compliance/AppPrivacyPolicyActivity.java
https://www.samsungapps.com/appquery/appDetail.as?appId=	com/ss/android/downloadlib/g/h.java
https://i.snssdk.com/	com/ss/android/downloadad/api/constant/AdBaseConstants.java
https://app.blokada.org/success	ui/ActivationViewModel$maybeRefreshAccountAfterUrlVisited$1.java
https://app.blokada.org/success	ui/ActivationViewModelKt.java
http://www.slf4j.org/codes.html#no_static_mdc_binder	org/slf4j/MDC.java

URL信息	Url所在文件
http://www.slf4j.org/codes.html#null_MDCA	org/slf4j/MDC.java
http://www.slf4j.org/codes.html	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#loggerNameMismatch	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#multiple_bindings	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#StaticLoggerBinder	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#null_LF	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#replay	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#substituteLogger	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#unsuccessfulInit	org/slf4j/LoggerFactory.java
http://www.slf4j.org/codes.html#version_mismatch	org/slf4j/LoggerFactory.java
https://go.blokada.org/forum	utils/Links.java
https://go.blokada.org/credits	utils/Links.java
https://go.blokada.org/donate	utils/Links.java
https://go.blokada.org/vpnrestore	utils/Links.java
https://go.blokada.org/introadblocking	utils/Links.java
https://go.blokada.org/kb_android	utils/Links.java
https://go.blokada.org/privacy	utils/Links.java
https://go.blokada.org/startonboot	utils/Links.java
https://go.blokada.org/terms	utils/Links.java

URL信息	Url所在文件
https://go.blokada.org/tunnelfailure	utils/Links.java
https://go.blokada.org/updated_android_slim	utils/Links.java
https://go.blokada.org/updated_android	utils/Links.java
https://go.blokada.org/dns	utils/Links.java
https://go.blokada.org/vpn	utils/Links.java
https://go.blokada.org/vpnperms	utils/Links.java
https://app.blokada.org/activate/	utils/Links.java
https://app.blokada.org/support?account-id=	utils/Links.java
https://app.blokada.org/activate	utils/Links.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling	io/reactivex/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://energized.pro/	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/spark/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/blu/hosts.txt	repository/PackDataSource.java

URL信息	Url所在文件
https://blokada.org/mirror/v5/energized/basic/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/adult/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/regional/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/social/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/energized/ultimate/hosts.txt	repository/PackDataSource.java
https://github.com/StevenBlack/hosts	repository/PackDataSource.java
https://blokada.org/mirror/v5/stevenblack/unified/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/stevenblack/fakenews/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/stevenblack/adult/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/stevenblack/social/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/stevenblack/gambling/hosts.txt	repository/PackDataSource.java
https://github.com/jerryn70/GoodbyeAds	repository/PackDataSource.java
https://blokada.org/mirror/v5/goodbyeads/standard/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/goodbyeads/youtube/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/goodbyeads/samsung/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/goodbyeads/xiaomi/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/goodbyeads/spotify/hosts.txt	repository/PackDataSource.java
https://github.com/AdAway/AdAway	repository/PackDataSource.java
https://blokada.org/mirror/v5/adaway/standard/hosts.txt	repository/PackDataSource.java

URL信息	Url所在文件
https://phishing.army/index.html	repository/PackDataSource.java
https://blokada.org/mirror/v5/phishingarmy/extended/hosts.txt	repository/PackDataSource.java
https://go.blokada.org/ddgtrackerradar	repository/PackDataSource.java
https://blokada.org/mirror/v5/ddgtrackerradar/standard/hosts.txt	repository/PackDataSource.java
https://github.com/anudeepND/blacklist	repository/PackDataSource.java
https://blokada.org/mirror/v5/blacklist/adservers/hosts.txt	repository/PackDataSource.java
https://blokada.org/mirror/v5/blacklist/facebook/hosts.txt	repository/PackDataSource.java
https://go.blokada.org/exodusprivacy	repository/PackDataSource.java
https://blokada.org/mirror/v5/exodusprivacy/standard/hosts.txt	repository/PackDataSource.java
https://blokada.org/api/v5/repo.json	repository/BlockaRepoRepositoryKt.java
https://api.blocka.net	repository/BlockaDataSource.java
https://blokada.org/api/v5/repo.json	repository/BlockaRepoRepository$fetch$2.java
https://anythingpriorityParseIntPoisonedexchangeselectormatchingservicesReadCodeKeyValueReservedprotocolinvalid.	lib/armeabi-v7a/libblocka_dns.so
https://set_hostE	lib/armeabi-v7a/libblocka_dns.so
http:////description()	lib/armeabi-v7a/libblocka_dns.so
http://https:///	lib/arm64-v8a/libblocka_dns.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libboringtun.so

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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference
android.permission.INTERACT_ACROSS_USERS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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
com.anguomob.adblock.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=anguo
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-01-20 06:12:35+00:00
Valid To: 2144-12-20 06:12:35+00:00
Issuer: CN=anguo
Serial Number: 0x31d6ca63
Hash Algorithm: sha256

md5: 55fd3556ce9f02326a473bfd51252cb4
sha1: 02cee04c70802663281aa2fbb9647154c43d6562
sha256: 8f59cb18bed8b8fce5d8c78245ac7df3bebc4b7ac948eba95c9acc5b4b24cda8
sha512: a2fc6899bd495f4fa0c72505ae27b6700e9f9d6c0084eba8668ab6007d9a8d448fb918a61269d3b0e05b8a9784c86ecad8d99af74eff863db582d47ad84d48ab
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 1a62ff9779100ae3366a986d755d7443e2813c6acc16f208406cf137eaf94de9

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"backup_key" : "AEdPqrEAAAAIOlPFZ6Ty7lGkyD2TXX8hYG7haLASV3_R5Edzig"
"pack_author" : "作者"
"read_private_str1" : "Be sure to fully read and understand the terms, including but not limited to: In order to provide you with business information and content sharing services, we need to collect your devic e information, operation logs and other personal information. Please review and agree before use"
"read_private_str2" : "with"
"read_private_str3" : "If you agree, click Agree and enter to start accepting our products and services. If you disagree, We will not be able to use our products and services 1, get mobile phone number and call status Statistics SDK use 2, get device location information Recommend you more needed content get current location weather information 3, read and write SDK permissions record user operation habits, Us er-friendly operation"
"read_private_title" : "User Security Policy"
"pack_author" : "作成者"

可能的敏感信息
"pack_author" : "Autor"
"pack_author" : "Автор"
"pack_author" : "Tekijä"
"pack_author" : "■■■■"
"pack_author" : "Autor"
"pack_author" : "Pembuat"
"pack_author" : "Autor"
"pack_author" : "المالك"
"pack_author" : "Auteur"
"pack_author" : "Yazar"
"pack_author" : "Autor"
"pack_author" : "Autor"
"pack_author" : "Autore"
"pack_author" : "Szerző"
"pack_author" : "Автор"
"pack_author" : "作者"
"pack_author" : "Autor"
"pack_author" : "作者"
"read_private_str1" : "一定要充分阅读和理解条款，包括但不限于:为了给您提供商业信息、共享内容等服务，我们需要收集您的设备信息、操作日志等个人信息。请在使用前查看并同意"

可能的敏感信息
"read_private_str2" : "与"
"read_private_str3" : "，如果你同意，点击"同意并进入"开始接受我们的产品和服务。若不同意，将无法使用我们的产品和服务 1、获取手机号码以及通话状态 友盟统计sdk使用 2、获取设备定位信息 推荐您更需要的内容 获取当前位置天气信息 3、读写sdk权限 记录用户操作习惯，方便用户操作"
"read_private_title" : "用户安全策略"
"pack_author" : "Author"

应用内通信

活动(ACTIVITY)	通信(INTENT)
ui.MainActivity	Schemes: https://, Hosts: app.blokada.org, Path Prefixes: /success,
ui.CommandActivity	Schemes: blocka://, Hosts: cmd, log, acc,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机 / Build.FINGERPRINT check Build.MANUFACTURER check possible Build.SERIAL check 编译器 / r8

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/1d7842c4752cfad2ae1855d9ce1d687a!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>Build.FINGERPRINT check
Build.MANUFACTURER check
Build.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
network interface name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
classes3.dex	壳列表 / 详细情况 反虚拟机: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check emulator file check 编译器: r8 without marker (suspicious)