南明离火
移动应用检测平台

ANDROID 静态分析报告

同じ市内の女の子 : v9.6.6

分析日期: 2025-04-09 11:03:14

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

i应用概览

文件名称:	同し市内の女の子.apk
文件大小:	89.12MB
应用名称:	同じ市内の女の子
软件包名:	com.wwzyjy.lkhbno
主活动:	org.telegram.ui.LaunchActivity
版本号:	9.6.6
最小SDK:	22
目标SDK:	31
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	51/100 (中风险)
跟踪器检测:	1/432
杀软检测:	恶意软件
MD5:	83d4c3dd43ffb468ede67210a295bd76
SHA1:	12334820f0681550ef4d2cc847376670cef1d898
SHA256:	e7ef9e0e29daf6c0768a1815d1b302efa6b8e33312223bd495d3c8c57479da93

⚠恶意软件家族信息

恶意家族	JiMaTongTrapTalk
描述信息	JiMaTongTrapTalk 是一款由南明离火平台追踪并命名的欺诈性应用程序，其核心基于 Telegram 构建。自 2019 年 7 月首次出现以来，该应用持续活跃，并通过多种手段实施恶意行为。其外观和功能模仿合法通讯软件及成人内容应用，诱导用户下载并使用，在此过程中窃取用户的个人和财务信息。从技术角度看，JiMaTongTrapTalk 通过多个云服务提供商隐藏其 C&C（命令与控制）服务器的真实位置，并采用国内广泛使用的安全加固工具（如 360 加固）以规避安全检测机制。在国内，该应用已导致大量用户受到侵害，衍生出数百个变种，对网络环境的安全稳定性和用户合法权益构成了严重威胁。其危害性不容忽视，需引起高度警惕，并采取有效措施防止其进一步传播与侵害。
C2服务器	目前只能观察到云服务器的 IP 地址，真实的 CC 服务器 IP 被隐藏。
凭证数据	升级会员：解锁高级权限
关联情报	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

分析结果严重性

高危	中危	信息	安全	关注
1	46	4	2	4

四大组件信息

Activity组件：16个，其中export的有： 13个
Service组件：30个，其中export的有： 14个
Receiver组件：23个，其中export的有： 3个
Provider组件：6个，其中export的有： 1个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=CN, ST=Shanghai, L=Shanghai, O=Company, OU=Android, CN=baby
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-22 12:30:34+00:00
有效期至: 2052-08-07 12:30:34+00:00
发行人: C=CN, ST=Shanghai, L=Shanghai, O=Company, OU=Android, CN=baby
序列号: 0x57853326
哈希算法: sha256
证书MD5: e1b3de628236b47b4ca7844a42ddcddb
证书SHA1: 6ab8a9e96f2c07f4b7baa84281d6d666366b999b
证书SHA256: 8bfc48d93d9e23773194864fbffe[illegible]4c554db76f65fd458996[illegible]af78[illegible]38
证书SHA512:
4a460adefd532d5eda2096f592f48a93f6c0f36eb491[illegible]49a867c50370bd4a73a2de1282043f11c641bb8ab3b8459c7e9362c32bd445e2c8e664e28acf03919403

公钥算法: rsa
密钥长度: 2048
指纹: 61110713cbcd341a2768d981[illegible]be03c9a77f52e917c013[illegible]4a6fe22abfb097a8
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
com.google.android.c2dm.permission.RECEIVE	普通	接收推送通知	允许应用程序接收来自云的推送通知。
com.wwzyjy.lkhbno.permission.MAPS_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.google.android.providers.gsf.permission.READ_GSERVICES	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.CALL_PHONE	危险	直接拨打电话	允许应用程序直接拨打电话。恶意程序会在用户未知的情况下拨打电话造成损失。但不被允许拨打紧急电话。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.READ_CALL_LOG	危险	读取通话记录	允许应用程序读取用户的通话记录
android.permission.READ_CLIPBOARD	未知	未知权限	来自 android 引用的未知权限。
android.permission.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
android.permission.INTERNET	危险	完全互联网访问	允许应用程序创建网络套接字。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡读取信息。
android.permission.GET_ACCOUNTS	普通	探索已知账号	允许应用程序访问帐户服务中的帐户列表。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加、删除帐户及删除其密码之类的操作。
android.permission.READ_PROFILE	危险	读取用户资料	允许应用程序读取用户个人信息。
android.permission.WRITE_SYNC_SETTINGS	危险	修改同步设置	允许应用程序修改同步设置。
android.permission.READ_SYNC_SETTINGS	普通	读取同步设置	允许应用程序读取同步设置，例如是否为 联系人 启用同步。
android.permission.AUTHENTICATE_ACCOUNTS	危险	作为帐户身份验证程序	允许应用程序使用 AccountManager 的帐户身份验证程序功能，包括创建帐户以及获取和设置其密码。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
android.permission.SYSTEM_ALERT_WINDOW	危险	弹窗	允许应用程序弹窗。 恶意程序可以接管手机的整个屏幕。
android.permission.READ_PHONE_STATE	危险	读取手机状态和标识	允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
android.permission.RECEIVE_BOOT_COMPLETED	普通	开机自启	允许应用程序在系统完成启动后即自行启动。这样会延长手机的启动时间，而且如果应用程序一直运行，会降低手机的整体速度。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

android.permission.USE_FINGERPRINT	普通	允许使用指纹	此常量在 API 级别 28 中已弃用。应用程序应改为请求USE_BIOMETRIC
android.permission.USE_BIOMETRIC	普通	使用生物识别	允许应用使用设备支持的生物识别方式。
android.permission.INSTALL_SHORTCUT	普通	允许在启动器中安装快捷方式	允许应用程序在Launcher中安装快捷方。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.android.launcher.permission.UNINSTALL_SHORTCUT	签名	删除快捷方式	这个权限是允许应用程序删除桌面快捷方式。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像。
android.permission.BLUETOOTH	危险	创建蓝牙连接	允许应用程序查看或创建蓝牙连接。
android.permission.MANAGE_OWN_CALLS	普通	使呼叫应用程序能够管理自己的呼叫	允许通过自我管理的ConnectionService API管理自己的调用的调用应用程序。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.READ_PHONE_NUMBERS	危险	允许读取设备的电话号码	允许读取设备的电话号码。这是READ PHONE STATE授予的功能的一个子集，但对即时应用程序公开。
com.sec.android.provider.badge.permission.READ	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	普通	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	普通	在应用程序上显示通知计数	在HTC手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	普通	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	普通	在应用程序上显示通知计数	在apex的应用程序启动图标上显示通知计数或徽章。
com.majeur.launcher.permission.UPDATE_BADGE	普通	在应用程序上显示通知计数	在solid的应用程序启动图标上显示通知计数或徽章。
com.huawei.android.launcher.permission.CHANGE_BADGE	普通	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.huawei.android.launcher.permission.READ_SETTINGS	普通	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.huawei.android.launcher.permission.WRITE_SETTINGS	普通	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。

本报告由南明离火移动安全分析平台生成

android.permission.READ_APP_BADGE	普通	显示应用程序通知	允许应用程序显示应用程序图标徽章。
com.oppo.launcher.permission.READ_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	普通	在应用程序上显示通知计数	在OPPO手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	未知权限	来自 android 引用的未知权限。
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	未知权限	来自 android 引用的未知权限。
com.android.vending.BILLING	普通	应用程序具有应用内购买	允许应用程序从 Google Play 进行应用内购买。
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.ACCESS_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS_COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
com.google.android.gms.permission.ACTIVITY_RECOGNITION	危险	允许应用程序识别身体活动	允许应用程序识别身体活动。
com.wwzyjy.lkhbno.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设置方面的数据。恶意应用程序可借此破坏您的系统配置。
com.asus.msa.SupplementaryDID.ACCESS	普通	获取厂商oaid相关权限	获取设备标识信息oaid，在华硕设备上需要用到的权限。
freemme.permission.msa	未知	未知权限	来自 android 引用的未知权限。

可浏览的Activity组件

ACTIVITY	INTENT
org.telegram.ui.LaunchActivity	Schemes: http://, https://, jmt://, c8gqdh://, xInstallScheme://, tg://, Hosts: telegram.me, telegram.dog, t.me, Mime Types: vnd.android.cursor.item/vnd.org.telegram.messenger.android.profile, */*,
org.telegram.ui.ShareActivity	Schemes: tgb://,

网络通信安全

序号	范围	严重级别	描述

证书安全分析

高危: 0 | 警告: 1 | 信息: 1

本报告由南明离火移动安全分析平台生成

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: 0 | 警告: 35 | 信息: 0 | 屏蔽: 0

序号	问题	严重程度	描述信息
1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
3	Service (org.telegram.messenger.GcmPushListenerService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
4	Service (org.telegram.messenger.GoogleVoiceClientService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
5	Activity (org.telegram.messenger.GoogleVoiceClientActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
6	Activity-Alias (org.telegram.messenger.DefaultIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity-Alias (org.telegram.messenger.VintageIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Activity-Alias (org.telegram.messenger.AquaIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
9	Activity-Alias (org.telegram.messenger.PremiumIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
10	Activity-Alias (org.telegram.messenger.TurboIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成

11	Activity-Alias (org.telegram.messenger.NoxIcon) 未被保护。 [android:exported=true]	警告	发现 Activity-Alias与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
12	Activity-Alias (org.telegram.ui.CallsActivity) 受权限保护，但是应该检查权限的保护级别。 Permission: android.permission.CALL_PHONE [android:exported=true]	警告	发现一个 Activity-Alias被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
13	Activity (org.telegram.ui.ShareActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
14	Activity (org.telegram.ui.ExternalActionActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
15	Activity (org.telegram.ui.ChatsWidgetConfigActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
16	Activity (org.telegram.ui.ContactsWidgetConfigActivity) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
17	Activity (org.telegram.messenger.OpenChatReceiver) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
18	Activity设置了TaskAffinity属性 (org.telegram.ui.VoIPPermissionActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
19	Activity设置了TaskAffinity属性 (org.telegram.ui.VoIPFeedbackActivity)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
20	Broadcast Receiver (org.telegram.messenger.SmsReceiver) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
21	Service (org.telegram.messenger.AuthenticatorService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
22	Service (org.telegram.messenger.ContactsSyncAdapterService) 未被保护。 [android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

23	Service (org.telegram.messenger.BringAppForegroundService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
24	Service (org.telegram.messenger.NotificationsService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
25	Service (org.telegram.messenger.VideoEncodingService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
26	Service (org.telegram.messenger.ImportingService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
27	Service (org.telegram.messenger.LocationSharingService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
28	Service (org.telegram.messenger.MusicPlayerService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
29	Service (org.telegram.messenger.MusicBrowserService) 未被保护。[android:exported=true]	警告	发现 Service与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
30	Service (org.telegram.messenger.voip.TelegramConnectionService) 受权限保护，但是应该检查权限的保护级别。Permission: android.permission.BIND_TELECOM_CONNECTION_SERVICE [android:exported=true]	警告	发现一个Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
31	Broadcast Receiver (org.telegram.messenger.RefererReceiver) 受权限保护，但是应该检查权限的保护级别。Permission: android.permission.INSTALL_PACKAGES [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
32	Content Provider (org.telegram.messenger.voip.CallNotificationSoundProvider) 未被保护。[android:exported=true]	警告	发现 Content Provider与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

33	Service (androidx.sharetarget.ChooserTargetServiceCompat) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_CHOOSER_TARGET_SERVICE [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
34	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	发现一个 Broadcast Receiver被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。
35	Service (com.google.android.gms.auth.api.signin.RevocationBoundService) 受权限保护, 但是应该检查权限的保护级别。 Permission: com.google.android.gms.auth.api.signin.permission.REVOCATION_NOTIFICATION [android:exported=true]	警告	发现一个 Service被共享给了设备上的其他应用程序，因此让它可以被设备上的任何其他应用程序访问。它受到一个在分析的应用程序中没有定义的权限的保护。因此，应该在定义它的地方检查权限的保护级别。如果它被设置为普通或危险，一个恶意应用程序可以请求并获得这个权限，并与该组件交互。如果它被设置为签名，只有使用相同证书签名的应用程序才能获得这个权限。

</> 安全漏洞检测

高危: **1** | 警告: **9** | 信息: **3** | 安全: **1** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
2	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限
3	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
4	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

5	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
6	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
7	如果一个应用程序使用WebView.loadDataWithBaseURL方法来加载一个网页到WebView，那么这个应用程序可能会遭受跨站脚本攻击	高危	CWE: CWE-79: 在Web页面生成时对输入的转义处理不恰当（'跨站脚本'） OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-6	升级会员：解锁高级权限
8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	此应用程序使用Safety Net API。	安全	OWASP MASVS: MSTG-RESILIENCE-7	升级会员：解锁高级权限
10	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
11	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
12	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

13	应用程序创建临时文件。敏感信息永远不应该被写进临时文件	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
14	此应用侦听剪贴板更改。一些恶意软件也会监听剪贴板更改	信息	OWASP MASVS: MSTG-PLATFORM-4	升级会员：解锁高级权限

动态库分析

序号	动态库	NX(堆栈禁止执行)	PIE	STACK CANARY(栈保护)	RELRO	RPATH（指定SO搜索路径）	RUNPATH（指定SO搜索路径）	FORTIFY(常用函数加强检查)	SYMBOLS STRIPPED（裁剪符号表）
1	arm64-v8a/libbeaconid.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用	True info 符号被剥离

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

2	arm64-v8a/libcloudclink-lib.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。	True info 符号被剥离
3	arm64-v8a/liblanguage_id_jni.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__vsnprintf_chk']	True info 符号被剥离

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

4	arm64-v8a/libqmp.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	False warning 二进制文件没有任何加固函数。加固函数提供了针对 glibc 的常见不安全函数（如 strcpy，gets 等）的缓冲区溢出检查。使用编译选项 -D_FORTIFY_SOURCE=2 来加固函数。这个检查对于 Dart/Flutter 库不适用。	True info 符号被剥离
5	arm64-v8a/libtmessages.45.so	True info 二进制文件设置了 NX 位。这标志着内存页面不可执行，使得攻击者注入的 shellcode 不可执行。	动态共享对象 (DSO) info 共享库是使用 -fPIC 标志构建的，该标志启用与地址无关的代码。这使得面向返回的编程 （ROP） 攻击更难可靠地执行。	True info 这个二进制文件在栈上添加了一个栈哨兵值，以便它会被溢出返回地址的栈缓冲区覆盖。这样可以通过在函数返回之前验证栈哨兵的完整性来检测溢出	Full RELRO info 此共享对象已完全启用 RELRO。 RELRO 确保 GOT 不会在易受攻击的 ELF 二进制文件中被覆盖。在完整 RELRO 中，整个 GOT（.got 和 .got.plt 两者）被标记为只读。	None info 二进制文件没有设置运行时搜索路径或 RPATH	None info 二进制文件没有设置 RUNPATH	True info 二进制文件有以下加固函数: ['__strlen_chk', '__FD_SET_chk', '__memcpy_chk', '__memset_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__vsnprintf_chk', '__memmove_chk', '__read_chk', '__strchr_chk']	True info 符号被剥离

行为分析

编号	行为	标签	文件
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成

00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00079	隐藏当前应用程序的图标	规避	升级会员：解锁高级权限
00146	获取网络运营商名称和 IMSI	电话服务 信息收集	升级会员：解锁高级权限
00078	获取网络运营商名称	信息收集 电话服务	升级会员：解锁高级权限
00038	查询电话号码	信息收集	升级会员：解锁高级权限
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00117	获取 IMSI 和网络运营商名称	电话服务 信息收集	升级会员：解锁高级权限
00033	查询IMEI号	信息收集	升级会员：解锁高级权限
00067	查询IMSI号码	信息收集	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00003	将压缩后的位图数据放入JSON对象中	相机	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00025	监视要执行的一般操作	反射	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00001	初始化位图对象并将数据（例如JPEG）压缩为位图对象	相机	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00206	检查视图的文本是否包含给定的字符串	无障碍服务	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00104	检查给定路径是否是目录	文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限
00064	监控来电状态	控制	升级会员：解锁高级权限
00102	将手机扬声器设置为打开	命令	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00052	删除内容 URI 指定的媒体（SMS、CALLLOG、文件等）	短信	升级会员：解锁高级权限
00065	获取SIM卡提供商的国家代码	信息收集	升级会员：解锁高级权限
00208	捕获设备屏幕的内容	信息收集 屏幕	升级会员：解锁高级权限
00202	打电话	控制	升级会员：解锁高级权限
00203	将电话号码放入意图中	控制	升级会员：解锁高级权限
00121	创建目录	文件 命令	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00137	获取设备的最后已知位置	位置 信息收集	升级会员：解锁高级权限

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

00115	获取设备的最后已知位置	信息收集 位置	升级会员：解锁高级权限
00080	将录制的音频/视频保存到文件	录制音视频 文件	升级会员：解锁高级权限
00101	初始化录音机	录制音视频	升级会员：解锁高级权限
00199	停止录音并释放录音资源	录制音视频	升级会员：解锁高级权限
00198	初始化录音机并开始录音	录制音视频	升级会员：解锁高级权限
00136	停止录音	录制音视频 命令	升级会员：解锁高级权限
00194	设置音源（MIC）和录制文件格式	录制音视频	升级会员：解锁高级权限
00090	设置录制的音频/视频文件格式	录制音视频	升级会员：解锁高级权限
00197	设置音频编码器并初始化录音机	录制音视频	升级会员：解锁高级权限
00138	设置音频源（MIC）	录制音视频	升级会员：解锁高级权限
00196	设置录制文件格式和输出路径	录制音视频 文件	升级会员：解锁高级权限
00133	开始录音	录制音视频 命令	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00002	打开相机并拍照	相机	升级会员：解锁高级权限
00195	设置录制文件的输出路径	录制音视频 文件	升级会员：解锁高级权限
00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00007	Use absolute path of directory for the output media file path	文件	升级会员：解锁高级权限
00204	获取默认铃声	信息收集	升级会员：解锁高级权限
00112	获取日历事件的日期	信息收集 日历	升级会员：解锁高级权限
00075	获取设备的位置	信息收集 位置	升级会员：解锁高级权限
00126	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限

本报告由南明离火移动安全分析平台生成

恶意软件常用权限	17/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.CALL_PHONE android.permission.READ_CALL_LOG android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.READ_PHONE_STATE android.permission.RECEIVE_BOOT_COMPLETED android.permission.CAMERA android.permission.REQUEST_INSTALL_PACKAGES android.permission.WRITE_SETTINGS
其它常用权限	12/46	com.google.android.c2dm.permission.RECEIVE android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.AUTHENTICATE_ACCOUNTS com.android.launcher.permission.INSTALL_SHORTCUT android.permission.BLUETOOTH android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_BACKGROUND_LOCATION com.google.android.gms.permission.ACTIVITY_RECOGNITION

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
usher.ttvnw.net	安全	否	**IP地址:** 18.154.206.23 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
bit.90932[illegible]vz	安全	否	No Geolocation information available.
telegram.me	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

attheme.org	安全	否	**IP地址:** 23.82.12.29 **国家:** 美国 **地区:** 佐治亚州 **城市:** 亚特兰大 **纬度:** 33.748795 **经度:** -84.387543 **查看:** Google 地图
desktop.telegram.org	安全	否	**IP地址:** 18.154.206.23 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
stripe.com	安全	否	**IP地址:** 35.167.74.49 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
www.aparat.com	安全	否	**IP地址:** 162.159.128.61 **国家:** 伊朗(伊斯兰共和国) **地区:** 德黑兰 **城市:** 德黑兰 **纬度:** 35.694241 **经度:** 51.421310 **查看:** Google 地图
ss3.4sqi.net	安全	否	**IP地址:** 149.154.167.99 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
api.twitch.tv	安全	否	**IP地址:** 18.65.25.59 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
crbug.com	安全	否	**IP地址:** 216.239.32.29 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
fragment.com	安全	否	**IP地址:** 149.154.167.99 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

coub.com	安全	否	**IP地址:** 52.26.14.11 **国家:** 俄罗斯联邦 **地区:** 桑克-彼得堡 **城市:** 圣彼得堡 **纬度:** 59.894440 **经度:** 30.264200 **查看:** Google 地图
api.stripe.com	安全	否	**IP地址:** 149.154.167.99 **国家:** 美国 **地区:** 俄勒冈 **城市:** 波特兰 **纬度:** 45.523460 **经度:** -122.676468 **查看:** Google 地图
tmessages2.firebaseio.com	安全	否	**IP地址:** 35.201.97.85 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
player.vimeo.com	安全	否	**IP地址:** 162.159.128.61 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
likeinstall.cn	安全	是	**IP地址:** 121.199.65.132 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
t.me	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
szcp.mxdx.net	安全	是	**IP地址:** 27.155.98.155 **国家:** 中国 **地区:** 福建 **城市:** 福州 **纬度:** 26.061390 **经度:** 119.306107 **查看:** 高德地图
tun-cos-1258244701.file.myqcloud.com	安全	是	**IP地址:** 219.159.86.56 **国家:** 中国 **地区:** 广西壮族 **城市:** 桂林 **纬度:** 25.281914 **经度:** 110.285187 **查看:** 高德地图

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

console.cloud.tencenct.com	安全	是	**IP地址:** 162.159.128.61 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
messenger.telegram.org	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
www.ietf.org	安全	否	**IP地址:** 104.16.45.99 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
telegram.org	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
aomediacodec.github.io	安全	否	**IP地址:** 185.199.108.153 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图
xinstall.top	安全	否	**IP地址:** 8.48.85.241 **国家:** 美国 **地区:** 路易斯安那州 **城市:** 门罗 **纬度:** 32.548328 **经度:** -92.045235 **查看:** Google 地图
translations.telegram.org	安全	否	**IP地址:** 149.154.167.99 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://turing.captcha.qcloud.com/TCaptcha.js	自研引擎-A

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://t.me/proxy? • https://t.me/socks?	org/telegram/messenger/SharedConfig.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• 209.244.0.4 • 216.146.35.35 • 36.99.163.69 • 114.98.229.75 • 185.228.169.168 • 77.88.8.8 • 199.85.127.10 • 80.80.80.80 • 77.88.8.2 • 120.71.147.135 • 1.71.130.123 • 113.24.58.36 • 198.54.117.10 • http://49.233.195.188:15000/api/uploadlog • http://console.cloud.tencenct.com:9999 • 9.9.9.9 • 199.85.126.10 • 116.8.104.127 • 216.146.36.36 • 149.112.112.112 • 118.122.77.126 • 64.6.64.6 • 185.228.168.168 • 8.8.4.4 • 8.8.8.8 • 127.0.0.1 • 115.239.250.104 • 114.67.65.53 • 94.140.15.15 • 203.57.5.59 • 36.99.168.155 • 121.228.46.194 • 64.6.65.6 • 121.204.188.189 • 106.58.222.161 • 113.219.242.125 • 182.151.21.10 • 208.67.220.123 • 168.95.1.1 • 36.99.153.178 • 218.30.118.6 • 94.140.14.14 • 208.67.222.222 • 209.244.0.3 • 4.2.2.2 • 4.2.2.1 • 208.67.220.220 • 80.80.81.81 • 195.46.39.39 • 106.42.28.198 • 116.198.53.199 • 140.246.31.209 • 59.80.22.232 • 77.88.8.88 • 116.198.35.13 • 125.74.29.120 • 208.67.222.123 • 114.67.182.19 • 1.0.0.1 • 1.71.14[illegible]60 • 1.1.1.1 • 168.95.192.1	cos/MyCOSService.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://play.google.com/store/account/subscriptions?sku=%s&package=%s	org/telegram/messenger/BillingController.java
• https://snowflake.qq.com/ola • https://test.snowflake.qq.com/ola	com/tencent/qimei/e/a.java
• https://telegram.org/dl	org/telegram/messenger/ContactsController.java
• https://api.stripe.com	com/stripe/android/net/StripeApiHandler.java
• 1.2.13.1	com/tencent/qimei/upload/BuildConfig.java
• https://xinstall.top • https://likeinstall.cn	com/shubao/xinstall/a/e/c.java
• https://stripe.com/docs/stripe.js	com/stripe/android/Stripe.java
• https://tun-cos-1258344701.file.myqcloud.com/fp.js • https://tun-cos-1258344701.file.myqcloud.com/my.html	com/tencent/qimei/s/c.java
• 10.0.2.15	org/telegram/messenger/EmuDetector.java
• https://tun-cos-1258344701.file.myqcloud.com/fp.js	com/tencent/qimei/s/a.java
• https://telegram.org/embed	org/telegram/ui/ArticleViewer.java
• https://fragment.com/username/ • https://fragment.com	org/telegram/ui/ChangeUsernameActivity.java
• https://t.me/botfather?start=	org/telegram/ui/ChatEditActivity.java
• https://fragment.com/username/	org/telegram/ui/ChannelCreateActivity.java
• https://fragment.com/username/	org/telegram/ui/ChatEditTypeActivity.java
• http://1.30.8.153:8088/images/yeastar.ico • http://1.15.81.219:8088/static/common/images/icon-play.png • http://bit.909321.xyz:8088/static/img/icons/favicon-32x32.png • http://console.cloud.tencent.com:9999 • http://1.15.89.53:8088/content/img/login-input-icon.png • http://szcp.mxdx.net:8088/cache/suzhiceping_exe/h3/res/__a406aaa462df6eec06e61d67.png • http://1.117.189.122:8088/truckmng/content/images/dsico.ico • http://27.151.172.32:8088/dist/oem/gocloud/favicon.ico • http://1.58.219.129:8088/source?get=vesn%20data.gif	org/telegram/ui/JMTFastShotManager.java
• https://ss3.4sqi.net/img/categories_v2/	org/telegram/ui/LocationActivity.java
• https://t.me/+ • https://t.me/joinchat/	org/telegram/ui/ManageLinksActivity.java
• https://telegram.org/deactivate?phone=	org/telegram/ui/PassportActivity.java
• https://fragment.com	org/telegram/ui/ProfileActivity.java
• https://t.me/proxy? • https://t.me/socks?	org/telegram/ui/ProxySettingsActivity.java

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

• https://t.me/$	org/telegram/ui/PremiumPreviewFragment.java
• https://t.me/+%s	org/telegram/ui/PrivacyControlActivity.java
• https://telegram.org	org/telegram/ui/ThemePreviewActivity.java
• https://attheme.org?slug=	org/telegram/ui/ActionBar/Theme.java
• https://telegram.org	org/telegram/ui/Cells/ThemePreviewMessagesCell.java
• https://messenger.telegram.org/	org/telegram/ui/Components/EmbedBottomSheet.java
• https://coub.com/api/v2/coubs/%s.json • http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s • https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s • https://player.vimeo.com/video/%s/config • https://api.twitch.tv/api/channels/%s/access_token • https://api.twitch.tv/kraken/streams/%s?stream_type=all	org/telegram/ui/Components/WebPlayerView.java
• https://play.google.com/store/apps/details?id=org.telegram.messenger	org/telegram/ui/Components/Premium/PremiumNotAvailableBottomSheet.java
• https://telegram.org/faq • https://telegram.me/telegramtips • https://telegram.org/faq#secret-chats • https://desktop.telegram.org/ • https://translations.telegram.org/%1$s/emoji • https://telegram.org/faq#passport • https://telegram.org • https://tmessages2.firebaseio.com • https://telegram.org/faq#q-i-have-a-new-phone-number-what-do-i-do • https://telegram.org/privacy	自研引擎-S
• 127.0.0.1 • 1.3.3.6	lib/arm64-v8a/libcloudclink-lib.so
• 28.8.8.8 • 127.0.0.1 • https://crbug.com/105375 • https://aomediacodec.github.io/av1-rtp-spec/#dependency-descriptor-rtp-header-extension • http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01	lib/arm64-v8a/libtmessages.45.so

FIREBASE数据库分析

标题	严重程度	描述信息
应用与Firebase数据库通信	信息	该应用与位于 https://tmessages2.firebaseio.com 的 Firebase 数据库进行通信
Firebase远程配置已禁用	安全	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/760348033671/namespaces/firebase:fetch?key=AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k ） 已禁用。响应内容如下所示: 响应码是 403

本报告由南明离火移动安全分析平台生成

第三方SDK

SDK名称	开发者	描述信息
腾讯灯塔 SDK	Tencent	灯塔（beacon）SDK 由腾讯灯塔团队开发，用于移动应用统计分析。
Bugly	Tencent	腾讯 Bugly，为移动开发者提供专业的异常上报和运营统计，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。
Golang	Google	Go 是一种开源编程语言，可轻松构建简单，可靠和高效的软件。
Qimei SDK	Tencent	提供终端设备的唯一标识 ID 体系服务，能精准的区分识别每一台终端设备，拥有海量级跨应用用户 ID 关系积累，以及实时的 ID 找回能力，应用于常规运营，结算场景。
Google Play Billing	Google	Google Play 结算服务可让您在 Android 上销售数字内容。本文档介绍了 Google Play 结算服务解决方案的基本构建基块。要决定如何实现特定的 Google Play 结算服务解决方案，您必须了解这些构建基块。
Google Sign-In	Google	提供使用 Google 登录的 API。
Google Play Service	Google	借助 Google Play 服务，您的应用可以利用由 Google 提供的最新功能，例如地图、Google+ 等，并通过 Google Play 商店以 APK 的形式分发自动平台更新。 这样一来，您的用户可以更快地接收更新，并且可以更轻松地集成 Google 必须提供的最新信息。
XPopup	li-xiaojun	内置几种了常用的弹窗，十几种良好的动画，将弹窗和动画的自定义设计的极其简单。
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件
Jetpack App Startup	Google	App Startup 库提供了一种直接，高效的方法来在应用程序启动时初始化组件。库开发人员和应用程序开发人员都可以使用 App Startup 来简化启动顺序并显式设置初始化顺序。App Startup 允许您定义共享单个内容提供程序的组件初始化程序，而不必为需要初始化的每个组件定义单独的内容提供程序。这可以大大缩短应用启动时间。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack AppCompat	Google	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack ShareTarget	Google	提供向后兼容性，可以将快捷方式用作直接共享目标。

邮箱

EMAIL	源码文件
support@stripe.com	com/stripe/android/net/StripeApiHandler.java
sms@telegram.org	org/telegram/ui/LoginActivity.java
sms@telegram.org	org/telegram/ui/PassportActivity.java
sms@stel.com	自研引擎-S
firebase-ml-android-sdk-releaser@otke9-20020a9d7309000b0[illegible]1914691.prod.google.com	lib/arm64-v8a/liblanguage_id_jni.so

追踪器

本报告由南明离火移动安全分析平台生成

名称	类别	网址
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

密钥凭证

可能的密钥
Xinstall推广SDK的=> "com.xinstall.APP_KEY" : "xInstallAppKey"
openinstall统计的=> "com.openinstall.APP_KEY" : "c8gqdh"
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k"
"UseProxySecret" : "Sleutel"
"UseProxySecret" : "Secret"
"CancelPasswordResetNo" : "NO"
"JMTUsername" : "Username"
"UseProxySecret" : "Segreto "
"PasswordCode" : "Code"
"RestorePasswordNoEmailTitle" : "Spiacenti"
"TypePrivateGroup" : "Privat"
"UsernameLinkActive" : "positif"
"PasswordOn" : "Ein"
"AbortPasswordMenu" : "Interromper"
"UsernameProfileLinkActive" : "positif"
"UseProxyPassword" : "Wachtwoord"
"YourPasswordSuccess" : "Keskkseban!"
"UseProxyUsername" : "Usuario"
"PasscodePassword" : "Senha"
"UseProxyUsername" : "Benutzername"
"firebase_database_url" : "https://fcmessages2.firebaseio.com"
"PasswordOff" : "No"
"CheckPasswordPerfect" : "Perfect!"
"UsernameProfileLinkActive" : "active"
"PaymentPasswordTitle" : "Password"
"ReportSpamUser" : "BLOQUEAR"

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

"TypePrivate" : "pribadi"
"PasswordOn" : "Activada"
"UseProxySecret" : "Clave"
"YourPasswordSuccess" : "Success!"
"UseProxySecret" : "Segredo"
"CancelPasswordResetNo" : "TIDAK"
"RestorePasswordNoEmailTitle" : "Sorry"
"NotificationHiddenChatUserName" : "Nutzer"
"PasswordOn" : "menyalakan"
"PasswordRecovery" : "Wachtwoordherstel"
"PasswordOff" : "Desactivada"
"LoginPassword" : "Senha"
"PasswordOff" : "Off"
"PasscodePassword" : "Wachtwoord"
"google_api_key" : "AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcboIR6k"
"Username" : "Gebruikersnaam"
"UsernameLinkActive" : "active"
"YourPasswordSuccess" : "Gelukt!"
"PaymentPasswordTitle" : "Senha"
"NotificationHiddenChatUserName" : "User"
"TypePrivate" : "Privat"
"PasswordCode" : "Codice"
"TypePrivateGroup" : "Privado"
"LoginPassword" : "Passwort"
"TypePrivate" : "Privado"
"google_app_id" : "1:760348033ca1:android:f6afd7b67eae3860"
"TypePrivateGroup" : "Private"
"CancelPasswordResetYes" : "Ya"
"PasswordOn" : "Aan"
"UseProxyPassword" : "Passwort"
"UseProxyUsername" : "Username"

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

"NotificationHiddenChatUserName" : "Usuario"
"PasswordOff" : "Uit"
"AutodownloadPrivateChats" : "Chats"
"NotificationHiddenChatUserName" : "Gebruiker"
"PasswordOn" : "On"
"PasscodePassword" : "Passwort"
"UseProxyPassword" : "Senha"
"UseProxyPassword" : "Password"
"NotificationHiddenChatUserName" : "Utente"
"ChannelPrivate" : "privat"
"ReportSpamUser" : "BLOKKEREN"
"PaymentPasswordTitle" : "Passwort"
"TypePrivateGroup" : "pribadi"
"PasswordOff" : "penutup"
"PaymentPasswordEmailTitle" : "Wiederherstellung"
"TypePrivate" : "Private"
"EncryptionKey" : "Encryptiesleutel"
"NotificationHiddenChatUserName" : "Pengguna"
"Username" : "Benutzername"
"PasscodePassword" : "Password"
"google_crash_reporting_api_key" : "AIzaSyA-t0jLPjUt2FxrA8VPK2LYHcYcboIR6k"
"PaymentPasswordEmailTitle" : "Herstel-e-mailadres"
"RestorePasswordNoEmailTitle" : "Desculpe"
"TerminateWebSessionStop" : "Cahaya%1$s"
"LoginPassword" : "Password"
"TypePrivate" : "Privato"
"UseProxyUsername" : "Gebruiker"
"Username" : "Username"
"PasswordOff" : "Desativada"
"CancelPasswordResetYes" : "YES"
"YourPasswordSuccess" : "Geschafft!"

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成

"TypePrivateGroup" : "Privato"
"LoginPassword" : "Wachtwoord"
"PasswordOff" : "Aus"
"PaymentPasswordTitle" : "Wachtwoord"
"YourPasswordSuccess" : "Fatto!"
"CheckPasswordPerfect" : "sempurna!"
"PasswordOn" : "Ativada"
"UseProxySecret" : "gram"
L3N5c3RlbS9ldGMvZXhjbHVkZWQtaW5wdXQtZGV2aWNlcy54bWw=
YW5kcm9pZC5oYXJkd2FyZS5ibHVldG9vdGg=
C71CAEB9C6B1C9048E6C522F70F13F73980D40238E3E21C14934D037563D930F48198A0AA7C14058229493D22530F4DBFA336F6E0AC925139543AED44CCE7C3720FD51F69458705AC68CD4FE6B6B13ABDC9746512969328454F18FAF8C595F642477FE96BB2A941D5BCD1D4AC8CC49880708FA9B378E3C4F3A9060BEE67CF9A4A4A695811051907E162753B56B0F6B410DBA74D8A84B2A14B3144E0EF1284754FD17ED950D595504B3DD46582DB1178D169C6BC465B0D6FF9CA3928FEF5B9AE4E418FC15E83EBEA0F87FA9FF5EED70050DED2849F47BF959D956850CE929851F0D8115F635B105EE2E4E15D04B2454BF6F4FADF034B10403119CD8E3B92FCC5B
Ldpv3DINc8b4Mg19EF0rkWBg7d2GJMJ3
bGV2ZWxfaXBhX3RzcmlmLnRjdWRvcnAub3I=
BvyoNmnTUIqvZufrqy6EPc/QFvgcZwweLUQZMPRjS0yO7ir5gj50Gm3WU1dVA==
ABVGDE2JZIQKLMNOPRSTUFHC34WXY9678
014b35b6184100b085b0d0572f9b5103
c06c8400-8e06-11e0-9cb6-0002a5d5c51b
bb392ec0-8d4d-11e0-a896-0002a5d5c51b
YW5kcm9pZC5oYXJkd2FyZS5jYW1lcmEuZmxhc2g=
A406AAA462DF6EEC06E61D6

免责声明及风险提示:

本报告由南明离火移动安全分析平台自动生成，内容仅供参考，不构成任何法律意见或建议。本平台对使用本产品及其内容所引发的任何直接或间接损失概不负责。本报告内容仅供网络安全研究，不得违反中华人民共和国相关法律法规。如有任何疑问，请及时与我们联系。

南明离火移动安全分析平台是一款专业的移动端恶意软件分析和安全评估框架。它能够执行静态分析和动态分析，深入扫描软件中中潜在的漏洞和安全隐隐患。

© 2025 南明离火 - 移动安全分析平台自动生成

本报告由南明离火移动安全分析平台生成
本报告由南明离火移动安全分析平台生成