南明离火
移动应用检测平台

ANDROID 静态分析报告

n n • v2.7.0

分析日期: 2025-04-15 02:58:54

应用概览

文件名称:	22.apk
文件大小:	49.53MB
应用名称:	n n
软件包名:	z0O4d.hPqO5om.RHOC9Or6m
主活动:	im.gukjhhafcz.ui.LaunchActivity
版本号:	2.7.0
最小SDK:	19
目标SDK:	28
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	44/100 (中风险)
跟踪器检测:	2/432
杀软检测:	9 个杀毒软件报毒
MD5:	7567d1b7f5c361b2c4d1dccea7a8e227
SHA1:	7349ca7d9a3af96332d8379e3cd7fd72aa14e0b1
SHA256:	c95c9d988b3a43a0d0db0bc90e1fc117eb274c7d11042e0cf8d419b3b659f33

恶意软件家族情报

恶意家族	Boomslang
描述信息	Boomslang（树蚺）是一个技术精湛的移动欺诈团伙，自2022年9月被首次进入安全研究人员的视野后始终保持着活跃的态势，不断更新逃避检测的技术手段。该团伙主要以开源的 Telegram Android 客户端代码作为其应用的核心框架。他们通过刷单、投资推广以及色情聊天等诱骗手段诱导用户安装恶意应用。在技术方面，该团伙采用DoH、防DDoS服务（如阿里游戏盾）以及OSS服务等一系列高级通信技术，这些技术手段的运用使其恶意应用能够有效地规避常规的检测机制与封堵措施，极大地增加了执法机构与安全防护团队追踪和防范其犯罪行为的难度，进一步凸显了该团伙在网络犯罪领域的专业能力以及对复杂网络环境的适应能力。
C2服务器	升级会员：解锁高级权限
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

分析结果严重性分布

高危	中危	信息	安全	关注
10	40	3	3	4

四大组件导出状态统计

Activity组件：16个，其中export的有： 3个
Service组件：26个，其中export的有： 13个
Receiver组件：19个，其中export的有： 8个
Provider组件：5个，其中export的有： 1个

应用签名证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=CN, ST=ZPgwIkSnSmtEyElNFIsOSWiAEgisQGgc, L=BaLsszAznonEoWMyaruvHirDmLSYLWvm, O=QsWGoAFzeDDeHksmlbfCHjyEkvLFYcSM, OU=GZAGnZKPbroeOASDuAsYljOuzwNWLQCO, CN=KDGntFNjFFItigHEWGjFQSenyiwhGAFY
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-20 18:01:46+00:00
有效期至: 2078-06-23 18:01:46+00:00
发行人: C=CN, ST=ZPgwIkSnSmtEyElNFIsOSWiAEgisQGgc, L=BaLsszAznonEoWMyaruvHirDmLSYLWvm, O=QsWGoAFzeDDeHksmlbfCHjyEkvLFYcSM, OU=GZAGnZKPbroeOASDuAsYljOuzwNWLQCO, CN=KDGntFNjFFItigHEWGjFQSenyiwhGAFY
序列号: 0x9cda0431e206d1d0
哈希算法: sha256
证书MD5: 64cde7cd2eda64a5d4d175a1b5d36e76
证书SHA1: 8a20848fc852e257af52528da8dbfd2c73be9a0f
证书SHA256: f3f1415c18a3e0591c05960e2ae4346113228b46f68d809ce1247764eae8090a
证书SHA512:
dd200ced31acbb9c12e2fb7b0dfa1...f8d1392d6cce9a2914...fe1f6e2c7e47b82b09a48821627f7c5480392a6c823a6cdb002f208d02b440d86dd7

公钥算法: rsa
密钥长度: 2048
指纹: abfb92a3570403477...5d8d79da04681339be7f
找到 1 个唯一证书

权限声明与风险分级

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。
im.gukjhhafcz.messenger.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。
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.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.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.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.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.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。
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.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.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.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。

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。
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。
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.READ_LOGS	危险	读取系统日志文件	允许应用程序从系统的各日志文件中读取信息。这样应用程序可以发现您的手机使用情况，这些信息还可能包含用户个人信息或保密信息，造成隐私数据泄露。
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.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.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.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.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.CHANGE_NETWORK_STATE	危险	改变网络连通性	允许应用程序改变网络连通性。
android.permission.REORDER_TASKS	危险	对正在运行的应用程序重新排序	允许应用程序将任务移至前端和后台。恶意应用程序可借此强行进入前端，而不受您的控制。
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.BROADCAST_PACKAGE_ADDED	签名	接收新增APP的通知	它允许一个应用程序接收到其他应用程序添加新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_CHANGED	签名	接收APP变化的通知	它允许一个应用程序接收到其他应用程序变化（安装、卸载、修改）的广播消息。
android.permission.BROADCAST_PACKAGE_INSTALL	签名	接收APP安装的通知	它允许一个应用程序接收到其他应用程序安装新包（即新安装的可执行文件）的广播消息。
android.permission.BROADCAST_PACKAGE_REPLACED	签名	接收APP替换的通知	它允许一个应用程序接收到其他应用程序被覆盖安装的广播消息。
android.permission.GET_TASKS	危险	检索当前运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
im.gukjhhafcz.messenger.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	普通	OPPO推送服务	OPPO推送服务正常工作所必需的，它允许应用接收来自OPPO推送系统的消息。
android.permission.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。

可浏览 Activity 组件分析

ACTIVITY	INTENT
im.gukjhhafcz.ui.LaunchActivity	Schemes: http://, https://, hchat://, rzrc91://, Hosts: m12345.cc, Mime Types: image/*, video/*, text/plain, */*, vnd.android.cursor.item/vnd.im.gukjhhafcz.messenger.android.profile,
im.gukjhhafcz.ui.ShareActivity	Schemes: hchat://,

网络通信安全风险分析

序号	范围	严重级别	描述

证书安全合规分析

高危: **0** | 警告: **1** | 信息: **1**

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 配置安全分析

高危: **7** | 警告: **28** | 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	应用程序具有网络安全配置 [android:networkSecurityConfig=@7F120005]	信息	网络安全配置功能让应用程序可以在一个安全的、声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	Service (im.gukjhhafcz.messenger.GcmPushListenerService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
4	Broadcast Receiver (com.google.android.gms.measurement.AppMeasurementReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
5	App 链接 assetlinks.json 文件未找到 [android:name=im.gukjhhafcz.ui.LaunchActivity] [android:host=http://m12345.cc]	高危	App Link 资产验证 URL （http://m12345.cc/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：None）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify=“true”] 启用验证来验证 App Link 网域。
6	App 链接 assetlinks.json 文件未找到 [android:name=im.gukjhhafcz.ui.LaunchActivity] [android:host=https://m12345.cc]	高危	App Link 资产验证 URL （https://m12345.cc/.well-known/assetlinks.json） 未找到或配置不正确。（状态代码：None）。应用程序链接允许用户从 Web URL/电子邮件重定向到移动应用程序。如果此文件丢失或为 App Link 主机/域配置不正确，则恶意应用程序可以劫持此类 URL。这可能会导致网络钓鱼攻击，泄露 URI 中的敏感数据，例如 PII、OAuth 令牌、魔术链接/密码重置令牌等。您必须通过托管 assetlinks.json 文件并通过 Activity intent-filter 中的 [android：autoVerify=“true”] 启用验证来验证 App Link 网域。
7	Activity (im.gukjhhafcz.ui.ShareActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。

本报告由南明离火移动安全分析平台生成

8	Activity (im.gukjhhafcz.ui.ExternalActionActivity) 未被保护。 存在一个intent-filter。	警告	发现 Activity与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Activity是显式导出的。
9	Activity (im.gukjhhafcz.ui.IntroActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
10	Activity (im.gukjhhafcz.messenger.OpenChatReceiver) 容易受到StrandHogg 2.0的攻击	高危	已发现活动存在 StrandHogg 2.0 栈劫持漏洞的风险。漏洞利用时，其他应用程序可以将恶意活动放置在易受攻击的应用程序的活动栈顶部，从而使应用程序成为网络钓鱼攻击的易受攻击目标。可以通过将启动模式属性设置为“singleInstance”并设置空 taskAffinity (taskAffinity="") 来修复此漏洞。您还可以将应用的目标 SDK 版本 (28) 更新到 29 或更高版本以在平台级别修复此问题。
11	Activity (im.gukjhhafcz.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。
12	Activity (im.gukjhhafcz.ui.PopupNotificationActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
13	Activity设置了TaskAffinity属性 (im.gukjhhafcz.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
14	Activity设置了TaskAffinity属性 (im.gukjhhafcz.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
15	Service (im.gukjhhafcz.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。
16	Service (im.gukjhhafcz.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。
17	Service (im.gukjhhafcz.messenger.AppChooserTargetService) 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。
18	Service (im.gukjhhafcz.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。
19	Service (im.gukjhhafcz.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。

20	Service (im.gukjhhafcz.messenger.WearDataLayerListenerService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
21	Service (im.gukjhhafcz.messenger.voip.AppConnectionService) 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。
22	Broadcast Receiver (im.gukjhhafcz.messenger.MusicPlayerReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
23	Broadcast Receiver (im.gukjhhafcz.messenger.voip.VoIPMediaButtonReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
24	Broadcast Receiver (im.gukjhhafcz.messenger.AppStartReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
25	Broadcast Receiver (im.gukjhhafcz.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。
26	Content Provider (im.gukjhhafcz.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。
27	Activity (im.gukjhhafcz.keepalive.OnePxActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
28	Service (im.gukjhhafcz.keepalive.ChannelService) 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 (im.gukjhhafcz.keepalive.DaemonService) 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 (im.gukjhhafcz.keepalive.ScheduleService) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.BIND_JOB_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 (im.gukjhhafcz.keepalive.MonitorReceiver) 未被保护。 存在一个intent-filter。	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Broadcast Receiver是显式导出的。
32	Broadcast Receiver (im.gukjhhafcz.keepalive.ScreenReceiver) 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。
33	Service (com.blankj.utilcode.util.MessengerUtils$ServerService) 未被保护。 存在一个intent-filter。	警告	发现 Service与设备上的其他应用程序共享，因此让它可以被设备上的任何其他应用程序访问。intent-filter的存在表明这个Service是显式导出的。
34	Activity (com.bjz.comm.net.premission.PermissionActivity) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
35	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。
36	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。

代码安全漏洞检测

高危: **3** | 警告: **10** | 信息: **2** | 安全: **2** | 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	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
3	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
4	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
5	应用程序使用带PKCS5/PKCS7填充的加密模式CBC。此配置容易受到填充oracle攻击。	高危	CWE: CWE-649: 依赖于混淆或加密安全相关输入而不进行完整性检查 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	升级会员：解锁高级权限
6	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
7	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
8	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密后写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
9	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
10	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

11	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
12	启用了调试配置。生产版本不能是可调试的	高危	CWE: CWE-919: 移动应用程序中的弱点 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-RESILIENCE-2	升级会员：解锁高级权限
13	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
14	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
15	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
16	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
17	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

Native 库安全加固检测

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/libtmessages.31.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: ['__FD_SET_chk', '__FD_ISSET_chk']	True info 符号被剥离

应用行为分析

编号	行为	标签	文件
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
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
00025	监视要执行的一般操作	反射	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
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
00204	获取默认铃声	信息收集	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

00036	从 res/raw 目录获取资源文件	反射	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
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
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
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
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
00033	查询IMEI号	信息收集	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
00191	获取短信收件箱中的消息	短信	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
00038	查询电话号码	信息收集	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
00192	获取短信收件箱中的消息	短信	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
00054	从文件安装其他APK	反射	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
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
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
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
00075	获取设备的位置	信息收集 位置	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
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
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
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
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
00052	删除内容 URI 指定的媒体（SMS、CALL_LOG、文件等）	短信	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
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
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
00056	修改语音音量	控制	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
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
00034	查询当前数据网络类型	信息收集 网络	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
00026	方法反射	反射	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
00092	发送广播	命令	升级会员：解锁高级权限

敏感权限滥用分析

类型	匹配	权限
恶意软件常用权限	16/30	android.permission.ACCESS_COARSE_LOCATION android.permission.ACCESS_FINE_LOCATION android.permission.MODIFY_AUDIO_SETTINGS android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.SYSTEM_ALERT_WINDOW android.permission.RECEIVE_BOOT_COMPLETED android.permission.REQUEST_INSTALL_PACKAGES android.permission.CALL_PHONE android.permission.RECORD_AUDIO android.permission.CAMERA android.permission.GET_ACCOUNTS android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.READ_PHONE_STATE android.permission.GET_TASKS
其它常用权限	13/46	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.AUTHENTICATE_ACCOUNTS com.android.launcher.permission.INSTALL_SHORTCUT android.permission.BLUETOOTH android.permission.READ_EXTERNAL_STORAGE android.permission.WRITE_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.REORDER_TASKS android.permission.FLASHLIGHT

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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
m.bjz.com	安全	否	No Geolocation information available.
api.twitch.tv	安全	否	**IP地址:** 3.167.138.124 **国家:** 美国 **地区:** 伊利诺伊州 **城市:** 芝加哥 **纬度:** 41.875771 **经度:** -87.620605 **查看:** Google 地图

impyq.gz.bcebos.com	安全	是	**IP地址:** 121.228.183.252 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
game.bjz.com	安全	否	No Geolocation information available.
api.stripe.com	安全	否	**IP地址:** 121.228.183.252 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.aparat.com	安全	否	**IP地址:** 121.228.183.252 **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
www.ntsc.ac.cn	安全	是	**IP地址:** 159.226.242.43 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
shibatch.sourceforge.net	安全	否	**IP地址:** 104.18.12.149 **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
game.imchat.im	安全	否	No Geolocation information available.
gukjhhafcz-48b[illegible]reaseio.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
stripe.com	安全	否	**IP地址:** 3.90.98.12 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
www.shareinstall.com.cn	安全	否	No Geolocation information available.

ip-api.com	安全	否	**IP地址:** 3.170.115.121 **国家:** 美国 **地区:** 北卡罗来纳州 **城市:** Skyland **纬度:** 35.483757 **经度:** -82.521996 **查看:** Google 地图
live.imchat.im	安全	否	No Geolocation information available.
usher.ttvnw.net	安全	否	**IP地址:** 3.170.115.121 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.783058 **经度:** -96.806503 **查看:** Google 地图
www.smpte-ra.org	安全	否	**IP地址:** 95.213.253.92 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
player.vimeo.com	安全	否	**IP地址:** 3.170.115.121 **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
ss3.4sqi.net	安全	否	**IP地址:** 151.101.2.132 **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
coub.com	安全	否	**IP地址:** 95.213.253.92 **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
m12345.cc	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图

translations.m12345.cc	安全	是	**IP地址:** 221.228.32.13 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图

URL 链接安全分析

URL信息	源码文件
• https://m12345.cc/deactivate?phone=	im/gukjhhafcz/ui/TwoStepVerificationActivity.java
• www.shareinstall.com.cn	im/gukjhhafcz/messenger/browser/Browser.java
• http://www.smpte-ra.org/schemas/2052-1/2010/smpte-tt	com/googlecode/mp4parser/authoring/tracks/SMPTETTTrackImpl.java
• https://m12345.cc/embed	im/gukjhhafcz/ui/ArticleViewer.java
• https://api.twitch.tv/api/channels/%s/access_token • https://api.twitch.tv/kraken/streams/%s?stream_type=all • https://player.vimeo.com/video/%s/config • http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s • https://coub.com/api/v2/coubs/%s.json • https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	im/gukjhhafcz/messenger/utils/PlayerUtils.java
• http://%s:%d/%s	com/danikula/videocache/Pinger.java
• http://m12345.cc • https://m12345.cc/authtoken/ • https://m12345.cc	im/gukjhhafcz/ui/hui/discovery/QrScanActivity.java
• https://m12345.cc/	im/gukjhhafcz/ui/components/URLSpanNoUnderline.java
• http://www.shareinstall.com.cn/js-test.html?appkey=7hda8k35whgpo4 • https://m12345.cc/install.html?appkey=7hda8k35whgpo4	im/gukjhhafcz/messenger/MessagesController.java
• https://stripe.com/docs/stripe.js	com/stripe/android/Stripe.java
• https://ss3.4sqi.net/img/categories_v2/	im/gukjhhafcz/ui/adapters/BaseLocationAdapter.java
• http://%s:%d/%s • 127.0.0.1	com/danikula/videocache/HttpProxyCacheServer.java
• https://m12345.cc/authtoken/ • https://openapi.baidu.com/oauth/2.0/token • https://vop.baidu.com/pro_api • https://m12345.cc • http://m12345.cc	im/gukjhhafcz/ui/ChatActivity.java
• www.shareinstall.com.cn	im/gukjhhafcz/ui/utils/QrCodeParseUtil.java

本报告由南明离火移动安全分析平台生成

• https://m12345.cc/proxy? • https://m12345.cc/socks?	im/gukjhhafcz/ui/ProxySettingsActivity.java
• http://www.ntsc.ac.cn	im/gukjhhafcz/ui/utils/timer/OrderCountDownHelper.java
• http://shibatch.sourceforge.net/	im/gukjhhafcz/ui/utils/translate/ssrc/SSRC.java
• https://api.stripe.com	com/stripe/android/net/StripeApiHandler.java
• https://api.twitch.tv/api/channels/%s/access_token • https://api.twitch.tv/kraken/streams/%s?stream_type=all • https://player.vimeo.com/video/%s/config • http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s • https://coub.com/api/v2/coubs/%s.json • https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	im/gukjhhafcz/ui/components/WebPlayerView.java
• https://vop.baidu.com/	com/bjz/comm/net/factory/ApiTranslateAudioFactory.java
• http://192.200.1.242:1999/ • http://192.168.1.4:20000/ • http://ip-api.com/json/ • https://game.imchat.im • http://m.bjz.com/ • https://impyq.gz.bcebos.com/ • http://game.bjz.com/ • https://106.13.253.35/ • https://106.13.253.90/ • https://live.imchat.im/	com/bjz/comm/net/UrlConstant.java
• https://impyq.gz.bcebos.com/	com/bjz/comm/net/utils/HttpUtils.java
• 36.255.220.245 • https://ikg143f.oss-accelerate.aliyuncs.com/andn3dUuW.txt • 192.200.1.117 • 192.168.1.184	im/gukjhhafcz/tgnet/NetworkConfig.java
• https://static-maps.yandex.ru/1.x/?l=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&lang=%s • https://static-maps.yandex.ru/1.x/?l=%.6f,%.6f&z=%d&size=%d,%d&l=map&scale=%d&pt=%.6f,%.6f,vkbkm&lang=%s	im/gukjhhafcz/messenger/AndroidUtilities.java
• https://m12345.cc/d	im/gukjhhafcz/messenger/ContactsController.java
• https://m12345.cc/deactivate?phone=	im/gukjhhafcz/ui/PassportActivity.java
• https://m12345.cc/privacy • https://m12345.cc/faq#passport • https://m12345.cc/faq#secret-chats • https://m12345.cc/faq • https://translations.m12345.cc/%1$s/emoji • https://gukjhhafc-48b0d.firebaseio.com	自研引擎-S
• 103.100.210.190	lib/arm64-v8a/libtmessages.31.so

Firebase 配置安全检测

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://gukjhhafcz-48b0d.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/194512522065/namespaces/firebase:fetch?key=AIzaSyC6uk1nvjb5BYzqEzgaWy_iTryf5373Nyw ） 已禁用。响应内容如下所示：
		{
		"state": "NO_TEMPLATE"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
阿里云游戏盾	Aliyun	游戏盾是通过封装登录器隐藏真实 IP，需要修改业务IP换成游戏盾 IP，然后在后台添加源 IP 和转发业务端口，玩家通过下载封装好的登录器进入游戏。采用多机房集群部署模式，节点切换无感知，加密所有连接，实现 CC 零误封，避免源 IP 泄漏，免疫 CC 与 DDOS 攻击。
AndroidUtilCode	Blankj	AndroidUtilCode 是一个强大易用的安卓工具类库，它合理地封装了安卓开发中常用的函数，具有完善的 Demo 和单元测试，利用其封装好的 APIs 可以大大提高开发效率。
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，并且可以更轻松地确保 Google 必须提供的最新信息。
EasyPermissions	Google	EasyPermissions 是一个包装器库，用于简化针对 Android M 或更高版本的基本系统权限逻辑。
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。
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。

邮箱地址敏感信息提取

EMAIL	源码文件
login@stel.com sms@stel.com	im/gukjhhafcz/ui/LoginActivity.java
sms@stel.com	im/gukjhhafcz/ui/CancelAccountDeletionActivity.java
sms@stel.com	im/gukjhhafcz/ui/ChangePhoneActivity.java
support@stripe.com	com/stripe/android/net/StripeApiHandler.java
login@stel.com sms@stel.com	im/gukjhhafcz/ui/hui/login/HloginActivity.java
login@stel.com	im/gukjhhafcz/ui/hui/login/LoginContronllerBaseActivity.java
sms@stel.com	im/gukjhhafcz/ui/PassportActivity.java

sms@stel.com	自研引擎-S

第三方追踪器检测

名称	类别	网址
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99

敏感凭证泄露检测

可能的密钥
openinstall统计的=> "com.openinstall.APP_KEY" : "rzrc91"
百度地图的=> "com.baidu.lbsapi.API_KEY" : "oYnHR3odlaw9KUleHaQP5BrTLivxSCz1"
谷歌地图的=> "com.google.android.maps.v2.API_KEY" : "AIzaSyA-t0jLPjUt2FxrA8VPK2EiYHcYcbcRck"
"PayPasswordReset" : "PayPasswordReset"
"TypePrivateGroup" : "Private"
"FindBackPassword" : "FindBack"
"google_api_key" : "AIzaSyC6uk1nvjb5BYzqEzgaWy_iTryf5373Nyw"
"YourPasswordSuccess" : "Success!"
"PayPassword" : "PayPassword"
"LoginPasswordReset" : "LoginPasswordReset"
"LoginPassword" : "Password"
"TypePrivate" : "Private"
"key_windowBackgroundGray" : "windowBackgroundGray"
"RestorePasswordNoEmailTitle" : "Sorry"
"UseProxyPassword" : "Password"
"TypePrivate2" : "Private"
"UseProxyUsername" : "Username"
"UserNameOrPhoneNumberSearch" : "Username"
"key_windowBackgroundWhite" : "windowBackgroundWhite"
"Username" : "Username"
"PayPasswordSetReminder" : "Tips"

"PasscodePassword" : "Password"
"PayPasswordSetting" : "PayPasswordSetting"
"baidu_map_key" : "oYnHR3odlaw9KUleHaQP5BrTLivxSCz1"
"key_walletDefaultBackground" : "walletDefaultBackground"
"Sessions" : "Sessions"
"yuncheng_app_key" : "-dSPyyHFK-C3oeMlwHTO+pKDObpgxP2MO7Uo2UCH0+AxbvSwOHSK26vswxbHqitmfpzvpr_umcseBVAt1Jhc*Z6pVK2u1Jycd5vGXSkkeksUjEvw7B1ab_L72k9kUie93wo9MKEFb_z5dDVJuy1dmCJ1lkTEoczXTFwV8KDvdhxGgMFuczwD-9Dky82dyNcpoA5r1MQjP9ySfU7B3*eJOvidufUoObTop+UEXpSPUk0S9Qz8Pt8bxT4nwwFJr18bwcZoeGyMLOYYBtZsWjTSuoCM-evTn1HNr6AjGt9PsQ2REKz14oSNoo4JB7gRopFVzhEnZ*wWTBKe3jbvAufn_d4Ur6uhiE34czv+fdJVeUHP"
"PasswordCode" : "Code"
"firebase_database_url" : "https://gukjhhafcz-48b0d.firebaseio.com"
"PaymentPasswordTitle" : "Password"
"google_app_id" : "1:194512522065:android:a3b6ee229cc1efe012e170"
"google_crash_reporting_api_key" : "AIzaSyC6uk1nvjb5BYzqEzgaWy_iTryf5373Nyw"
"UseProxySecret" : "Secret"
C71CAEB9C6B1C9048E6C522F70F13F73980D40238E3E21C14934D037563D930F48108A0AA7C14058229493D22530F4DBFA336F6E0AC925139543AED44CCE7C3720FD51F69458705AC68CD4FE6B6B13ABDC9746512969328454F185AF8C595F642477FE96BB2A941D5BCD1D4AC8CC49880708FA9B378E3C4F3A9060BEE67CF9A4A4A695811051907E162753B56B0F6B410DBA74D7A34B2A14B3144E0EF1284754FD17ED950D5965B4B9DD46582DB1178D169C6BC465B0D6FF9CA3928FEF5B9AE4E418FC15E83EBEA0F87FA9F5FED70050DED2849F47BF959D956850CE929851F0D8115F635B105EE2E4E15D04B2454BF6F4FADF034B10403119CD8E3B92FCC5B
ABVGDE2JZIQKLMNOPRSTUFHC34WXY9678
9A04F079-9840-4286-AB92-E65BE0885F95
pE5eNoBQIFVcd9IEuylhvopfgS1RSj5C
fb9f0bb7fdd0760c354cc3d80cecb1d9
f180c508-f49a-40bd-b8ac-5057ce0aff6
A2B55680-6F43-11E0-9B8F-0002A5D5C51B
e283aac0-7c0f-4f2e-bcf7-90acc19903ed

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。