南明离火
移动应用检测平台

ANDROID 静态分析报告

蚂蚁优借 • v4.1.2

分析日期: 2025-04-08 10:27:42

应用概览

文件名称:	蚂蚁优借_dntcle.nciiac.ghvicr_bfeffb934c22b6d7df307692f8137aa9.apk
文件大小:	19.3MB
应用名称:	蚂蚁优借
软件包名:	dntcle.nciiac.ghvicr
主活动:	com.mayiyoujiefsd.ui.activitys.JDXF0ACT
版本号:	4.1.2
最小SDK:	22
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:	45/100 (中风险)
跟踪器检测:	1/432
杀软检测:	恶意软件
MD5:	07614f5f0ea2b453c167508714f12993
SHA1:	51c053fa52938907fab254de0c3b00e3d784e9af
SHA256:	c145a0a4f7207d0ce7e7b0079ce576fc318850a90897ade87feebab10205f76a

恶意软件家族情报

恶意家族	Cyanopica
描述信息	Cyanopica（灰喜鹊）家族是南明离火平台识别出并命名的一系列仿冒金融应用的诈骗软件，专门设计来诱骗用户安装并窃取他们的个人及财务信息。这些应用通过加密技术将URL隐藏在云端（例如myqcloud、阿里云OSS、亚马逊云等）中，以掩盖真实的服务器地址，从而巧妙地避开安全检测和追踪。此外，Cyanopica家族可能还实施了线路冗余策略，进一步增强了其隐蔽性和操作的复杂性，对用户的网络安全和财产安全构成了显著威胁。
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
5	16	2	2	4

四大组件导出状态统计

Activity组件：352个，其中export的有： 1个
Service组件：5个，其中export的有： 1个
Receiver组件：2个，其中export的有： 2个
Provider组件：7个，其中export的有： 0个

应用签名证书信息

二进制文件已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: None
主题: C=anvyobvttkfgd, ST=dvqhnubapekwn, L=tgaulynjhcfoa, O=fig1742295586257, OU=qvm1742295586257, CN=TG@apken888
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-18 10:59:46+00:00
有效期至: 2075-03-06 10:59:46+00:00
发行人: C=anvyobvttkfgd, ST=dvqhnubapekwn, L=tgaulynjhcfoa, O=fig1742295586257, OU=qvm1742295586257, CN=TG@apken888
序列号: 0x7c31077c
哈希算法: sha1
证书MD5: 0b867e6231c21563a8138462e334c0cf
证书SHA1: 14bea58e26a35cc38534f692e729c90101dff09c
证书SHA256: c3c96d4433a5ec1b5c10cc479478ab1cf08b94f15ed177c0c114e832f17827bd
证书SHA512:
43a2bb2e1aee56eac37eb765b87379056bab6f9c95f17c174b2b0ea0639781ab54f8599c32740eb8e529449976c50f7e91a7a3086673bed5e0812e71a8fe1f185

公钥算法: rsa
密钥长度: 1024
指纹: 68a64c936e6cd8e4e77791b32f6afc005636d33557130e8f95b65315fca830
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
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.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.CHANGE_WIFI_STATE	危险	改变Wi-Fi状态	允许应用程序改变Wi-Fi状态。
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.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。

本报告由南明离火移动安全分析平台生成

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_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.READ_SMS	危险	读取短信	允许应用程序读取您的手机或 SIM 卡中存储的短信。恶意应用程序可借此读取您的机密信息。
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.WRITE_CALL_LOG	危险	写入通话记录	允许应用程序写入（但不读取）用户的通话记录数据。
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.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.READ_EXTERNAL_STORAGE	危险	读取SD卡内容	允许应用程序从SD卡中读取信息。
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.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.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.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_MEDIA_VISUAL_USER_SELECTED	危险	允许从外部存储读取用户选择的图像或视频文件	允许应用程序从用户通过权限提示照片选择器选择的外部存储中读取图像或视频文件。应用程序可以检查此权限以验证用户是否已选择使用照片选择器，而不是授予对 READ_MEDIA_IMAGES 或 READ_MEDIA_VIDEO 的访问权限。它不会阻止应用程序手动访问标准照片选择器。应与 READ_MEDIA_IMAGES 和/或 READ_MEDIA_VIDEO 一起请求此权限，具体取决于所需的媒体类型。
android.permission.READ_MEDIA_IMAGES	危险	允许从外部存储读取图像文件	允许应用程序从外部存储读取图像文件。
android.permission.READ_MEDIA_VIDEO	危险	允许从外部存储读取视频文件	允许应用程序从外部存储读取视频文件。
android.permission.READ_MEDIA_AUDIO	危险	允许从外部存储读取音频文件	允许应用程序从外部存储读取音频文件。

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: 0 | 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: **0** | 警告: **5** | 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	Broadcast Receiver (com.base.commonlibrary.netstate.NetworkStateReceiver) 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。
3	Broadcast Receiver (com.mayiyoujiefsd.gzd.FZGBReceiver) 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。
4	Activity (com.sina.weibo.sdk.share.ShareResultActivity) 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。
5	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: **5** | 警告: **9** | 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	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
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

本报告由南明离火移动安全分析平台生成

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
5	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
6	不安全的Web视图实现。Web视图忽略SSL证书错误并接受任何SSL证书。此应用程序易受MITM攻击	高危	CWE: CWE-295: 证书验证不恰当 OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	升级会员：解锁高级权限
7	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
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。敏感信息也应加密并写入数据库	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	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
10	此应用程序可能会请求root（超级用户）权限	警告	CWE: CWE-250: 以不必要的权限执行 OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
11	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
12	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

13	使用弱加密算法	高危	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
15	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
16	该文件是World Writable。任何应用程序都可以写入文件	高危	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
17	已启用远程WebView调试	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
18	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

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/libfacedevice.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: ['__vsprintf_chk', '__memmove_chk', '__strchr_chk', '__memset_chk', '__memcpy_chk', '__strcpy_chk', '__vsnprintf_chk', '__strlen_chk']	True info 符号被剥离
2	arm64-v8a/libtoyger.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

应用行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	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
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

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
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
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
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
00091	从广播中检索数据	信息收集	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
00012	读取数据并放入缓冲流	文件	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
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
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
00192	获取短信收件箱中的消息	短信	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
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
00054	从文件安装其他APK	反射	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
00087	检查当前网络类型	网络	升级会员：解锁高级权限
00103	检查活动网络类型	网络	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
00002	打开相机并拍照	相机	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
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
00153	通过 HTTP 发送二进制数据	http	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
00033	查询IMEI号	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
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
00130	获取当前WIFI信息	WiFi 信息收集	升级会员：解锁高级权限
00147	获取当前位置的时间	信息收集 位置	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
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
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限
00062	查询WiFi信息和WiFi Mac地址	WiFi 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
00082	获取当前WiFi MAC地址	信息收集 WiFi	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	9/30	android.permission.READ_PHONE_STATE android.permission.WRITE_CONTACTS android.permission.READ_CONTACTS android.permission.READ_SMS android.permission.CAMERA android.permission.WRITE_CALL_LOG android.permission.READ_CALL_LOG android.permission.RECORD_AUDIO android.permission.REQUEST_INSTALL_PACKAGES
其它常用权限	11/46	android.permission.INTERNET android.permission.ACCESS_WIFI_STATE android.permission.CHANGE_WIFI_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.ACCESS_NETWORK_STATE android.permission.READ_EXTERNAL_STORAGE android.permission.CHANGE_NETWORK_STATE android.permission.FOREGROUND_SERVICE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO android.permission.READ_MEDIA_AUDIO

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
nice800.com	安全	是	**IP地址:** 43.132.110.135 **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
service.weibo.com	安全	是	**IP地址:** 49.7.37.75 **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
www.beizhuabao.com	安全	否	No Geolocation information available.
ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	安全	是	**IP地址:** 27.155.119.180 **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
jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com	安全	是	**IP地址:** 3.5.237.170 **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
i.open.t.sina.com.cn	安全	否	**IP地址:** 10.7.129.96 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图

URL 链接安全分析

URL信息	源码文件

• https://y.qq.com/portal/player.html • http://h.xiami.com/ • https://c.y.qq.com/v8/fcg-bin/fcg_v8_album_info_cp.fcg • https://music.163.com/ • http://music.163.com/discover • https://www.xiami.com/song/ • https://c.y.qq.com • http://acs.m.xiami.com/h5 • https://u.y.qq.com • https://music.163.com • http://feross.org • http://y.gtimg.cn/music/photo_new/T001R300x300M000 • https://y.qq.com/n/yqq/song/ • http://api.xiami.com • https://y.gtimg.cn/music/photo_new/T002R300x300M000 • http://music.163.com	自研引擎-A
• http://www.beizhuabao.com	d/n/b/d/a/a.java
• http://www.beizhuabao.com	d/n/b/d/a/b.java
• https://service.weibo.com/share/mobilesdk_uppic.php	d/r/a/a/a/d.java
• https://plus.google.com/	d/k/a/c/c/k/s1.java
• http://i.open.t.sina.com.cn/mobilesdk/sendmessage.php	d/r/a/a/a/c.java
• https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com • https://zxcvljalksjfnv.oss-accelerate.aliyuncs.com • https://ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com	d/n/b/d/a/e.java
• https://android-downloadoss-cn-hangzhou.aliyuncs.com/domai0dsfnname/5100sdfh0635.text/	d/n/b/d/a/d.java
• http://mdc.html5.qq.com/mh?channel_id=50079&u=	d/s/b/b/p/e.java
• https://dlib-shanghai-aliyun-cloudauth-oss.cn-shanghai.aliyuncs.com/model/toyger.face.dat • https://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png	d/h/a/n/k.java
• https://service.weibo.com/share/mobilesdk.php	d/r/a/a/i/c/d.java
• http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_debugplugin_debugplugin.tbs	d/s/b/c/m.java
• https://accounts.google.com/o/oauth2/revoke?token=	d/k/a/c/a/a/e/c/f.java
• https://n.cz200.com/	com/mayiyoujiefsd/ui/activitys/MT10ACT.java
• www.qq.com • http://pms.mb.qq.com/rsp204	d/s/b/b/w.java

• http://cfg.imtt.qq.com/tbs?v=2&mk=	d/s/b/c/w.java
• https://nice800.com	com/mayiyoujiefsd/ui/activitys/MT7ACT.java
• https://render.alipay.com/p/yuyan/180020010001208736/aliyunfacewelcome.html	自研引擎-S

第三方 SDK 组件分析

SDK名称	开发者	描述信息
金融级实人认证 SDK	Alibaba	金融级实人认证服务搭载真人检测和人脸比对等生物识别技术，配合权威数据源验证，可快速校验自然人的真实身份。
Fresco	Facebook	Fresco 是一个用于管理图像及其使用的内存的 Android 库。
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。
C++ 共享库	Android	在 Android 应用中运行原生代码。
IJKPlayer	Bilibili	IJKPlayer 是一款基于 FFmpeg 的轻量级 Android/iOS 视频播放器，具有 API 易于集成、编译配置可裁剪、支持硬件加速解码、DanmakuFlameMaster 架构清晰、简单易用等优势。
微博 SDK	Weibo	微博 Android 平台 SDK 为第三方应用提供了简单易用的微博 API 调用服务，使第三方客户端无需了解复杂的验证机制即可进行授权登陆，并提供微博分享功能，可直接通过微博官方客户端分享微博。
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。
AgentWeb	Justson	AgentWeb 是一个基于的 Android WebView ，极度容易使用以及功能强大的库，提供了 Android WebView 一系列的问题解决方案，并且轻量和极度灵活。
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。
Picasso	Square	一个强大的 Android 图片下载缓存库。
FileDownloader	LingoChamp	Android 文件下载引擎，稳定、高效、灵活、简单易用。

第三方追踪器检测

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

敏感凭证泄露检测

可能的密钥
凭证信息=> "com.amap.com.mayiyoujiefsd.mjyp.app.api.v2.apikey" : "0bsdfvdd0"

3082023f308201a8a00302010202044c46914a300d06092a864886f70d01010505003064310b3009060355040613023836311030 0e060355040813074265696a696e673110300e060355040713074265696a696e673110300e060355040a130754656e63656e74310c300a060355040b1303575344311130 0f060355040313086d75656c6d6f301e170d3130303732313036313835305a170d3430303731333036313835305a3064310b3009060355040613023836311030 00e060355040813074265696a696e673110300e060355040713074265696a696e673110300e060355040a130754656e63656e74310c300a060355040b13 03575344311130 0f060355040313086d75656c6d6f30819f300d06092a864886f70d01010105000381800300818902818100c209077044bd0d63ea00 ede5b839914cabcc912a87f0f8b390877e0f7a2583f0d5933443c40431c35a4433bc4c965800141961adc44c9625b1d321385221fd097e5bdc2f44a1840d64 3ab59dc070cf6c4b4b4d98bed5cbb8046e0a7078ae134da107cdf2bfc9b440fe5cb2f7549b44b73202cc6f7c2c55b8cfb0d333a021f01f0203010001300d060 92a864886f70d01010505000381810 0b007db9922774ef4ccfee81ba514a8d57c410257e7a2eba64bfa17c9e690da08106d32f637ac41fbc9f205176c71bde 238c872c3ee2f8313502bee44c80288ea4ef377a6f2cdfe4d3653c145c4acfedbfbadea23b559d41980cc3cdd35d79a68240693739aabf5c5ed26148756cf882 64226de394c8a24ac35b712b120d4d23a

308203773082025fa003020102020448bb959d300d06092a864886f70d01010b0500306b310b3009060355040613026 3112301006035504081309477 5616e67646f6e673111300f060355040713085368656e7a68656e3110300e060355040a130754656e63656e74310c300a060355040b13034c4947311530 306035504031302 30603550403130c4d696e676875204875616e673020170d3136303532313039353730335a180f323037313032323230393537303 5a306b310b30090603 5504061302636e311230100603550408130947756 16e67646f6e673111300f060355040713085368656e7a68656e3110300e060355040a130754656e63656 6e74310c300a060355040b13034d4947311530130603550403130c4d696e676875204875616e6730820122300d06092a864886f70d01010105000382010f 003082010a02820101008c58deabefe95f699c6322f9a75620873b490d26520c7267eb8382a91da625a5876b2bd617116e040a371c4f88c988c1ba73052ca aa9964873c94b7755c3429fca47a6677229fb2e72908d3b17df82f1ebe70447b94c1e5b0a763dad894831218032266732506f01e423e0409ef3a59e5c0e0b 9c765a2322699a2dec2d4dbe58ec15f41752516192169d9596169f5bf08eaf8aab9893240ad679e82fc92b97d2a 8021dc5a752f0a69437ea603c541e6 753cea52dbc8e8043fe21fd5da46066c92e0714905dfad3116f35aca52b13871c57481459aa4ca255a6482ba972bd af90d0d2c21a57ef65376bbd4ce7078 e6047060640669f3867fdc69fbb750203010001a321301f301d0603551d0e0416041450fb9b6362e829797 f79ca55e6d5e082e93ff33 d06092a864886f 70d01010b05000382010100 4952ffbfba7c00ee9b84f44b05ec62bc2400dc769fb2e83f80395e3fbb54e4 56a165 27413d144f42bf8f2 a433c42a7a732d e9d5124df906c6d728e75ca94eefc918080876bd3ce6cb5f7f2d9cc8d8e708033afc1295c7f347fb2d 8b1e4a79220e9552171d5 5f8f5 cf4c6478cc41dc e24cbe942305757488d37659d3265838ee54ebe44fccbd1bec93d809f950034f5ef292f20179554 2 856c03b4d44997fcb9b 16a49218fce0e2e6bfe 1fd4aa0ab39f548344c244c171c203baff1a730883aaf4506b6865a45c3c9aba40c6326d4152b6ce c0c 864bec1d6422e83dad949 83fb252b4bfb30d3 a6badf996099793e11f9af618d

30820253308201bca00302010202044bbb0361300d06092a864886f70d01010505003 306d310 300c060355040 13054368696e61310f300d06035504080c 06e58c97e4baac310f300d06035504070c06e58c97e4baac310f300d060355040a0c06e885bee8aeaf311b3019060355040b0c12e697a0e7babfe4b89ae58 aa1e7b3bbe7bb9f310b3009060355040313025151 3020170d313030343036 3 343831375a180f323238 4 313230303934383 1375a306d310e300c06 035504061305436869 6e61310f300d06035504080c06e58c97e4baac310f300d060355040a0c06e885bee8aeaf31 1b3019060355040b0c12e697a0e7babfe4b89ae58aa1e7b3bbe7bb9f 10b3009060355040313025151 30 19f300d06092a864886f70d010101050003818d 0030818902818100a15e9756216f694c5915e0b529095254367c4 54 af 07ae13488d946615a5 ddc 1a415f717d019edc6d30b9603d3e2a7b3de0ab7e0 cf52dfee39373bc472fa997027d798d59f81d525a69ecf156e885fd1e 909 4386b2230cc90e3b7 dc 603ddcf4c40bdc72f22db0f216a99c371d3bf89cba6 578c60699e8a0d536950203010001300d06092a864886f70d 0101 0505000381810094a9b 0e80691645dd42d6611775a855f71bcd4d77cb60a8e2940403 5a5e00b21bcc5d4a562482126bd91b6b0e50709377ceb9efa c 1fd12cc8b16afd9a159f350 b 0b14204ff065d843832720702e28b41491fbc3a205f5f2f42 526d67f17614d8a974de6487b2c866efede3b4e49a0 916 aa3c 336fd2ee1b162 52049

b20292cc45269854c712

ab05c5fe1172477aa023e3046a6abbd2

MIGfMA0GCSqGSIb3DQEBAQUAA4GN DZB QKBgQC3DtFIIG5OhLgY 1A GAx4DAhLyag2HSd2lsr1L66hH9SdefhaknsujWnumk+yNMYlQFdDnJ1Z8A4kj6zL JYRnNLyUeU0tI9uMlPr6AGbdia 5PoK0YXJY6pxEw3w55oozn MswIRyv93o8fBKWx/7mEnsrayE8VITzHroIuQIDAQAB

30820239308201a2a003020102020044c96f48f300d06092a864886f70d01010505003060310b3009060355040613024e310b3009060355040813024744 3112301006035504073009477 5616e677a686f753110300e060355040a130754656e63656e74310b3009060355040b1302334731111300f06035504031308 57696c736f6e5753020170d3130303932303035 3 3334335a180f323036353036323330353433343335a3060310b3009060355040613024e310b300906 0355040813024744311230100603550407130947756 16e677a686f753110300e060355040a130754656e63656e74310b3009060355040b1302334731113 00f060355040313085769 6c736f6e5753020119300d06092a864886f70d01010105000381 8d0030818902818100b56e79dbb1185a79e52d792bb3d0bb3da 8010d9b 9 a32ec69f7dc5ad66ab6bd 2f6a ed285dd2358f28b72a468be7c10a2ce30c4c27323ed4edcc936080e5bedc2cbbca0b7e879c08a631182793f 44bb3ea284 79b263410c298e5f6831 2c9702ba4a74e2ccfc9ef857f12201451602fc8e774ac59d6398511586c83d1d0203010001300d06092a864886f70 d01010505000381810024756 6b 8d8786b89053580294884038 7d06b1692ff3ea47ef4c435719ba1865b81e6bfa6293ce31747c3cd6b34595b485cc15 63fd90107ba5845c28b95c791 8f0d c288940395bc10f92f2b69d8dc410999deb38900974ce9984b678030edfba8816582f56160d87e38641288d8588d2a 31e20b89f223d788dd3 c9 8

16dac3c707f44f 4b 2c879 41440568

308202eb30820254a00302010202044d36f7a4300d06092a864886f70d01010505003081b9310b3009060355040613023836311230100603550408130947756 16e67646f6e673111300f06035504071308536865 6e7a68656e3135303360355040a132c54656e63656e7420546563686e6f6c6f6779285368656e7a68656e2920436f6d70616e79204c696d69746564313a3038060355040b133154656e63656e74204775616e677a686f752052657365617263682061 6e6420446576656c6f706d656e742043656e7465723110300e060355040313075 4656e63656e7430819f300d06092a864886f70d010101050003818d00308189028181 00c05f34b231b083fb1323670bfbe7bdab40c0c0a6efc87ef2072a1ff0d60cc67c8edb0d0847f210bea6cbfaa241be70c86daf56be08b723c859e52428a064555d80db448cdcacc1aea2501eba06f8bad12a4fa49d85cacd7abeb68945a5cb5e061629b52e3254c373550ee4e40cb7c8ae6f7a8151ccd8df582d446f39ae0c5e930203010001300d06092a864886f70d0101050500038181009c8d9d7f2f908c42081b4c764c377109a8b2c70582422125ce545842d5f520aea69550b6bd8bfd94e987b75a3077eb04ad341f481aac266e89d3864456e69fba13df018acdc168b9a19dfd7ad9d9cc6f6ace57c746515f71234df3a053e33ba93ece5cd0fc15f3e389a3f365588a9fcb439e069d3629c4782a13fff7b891499
fd4ddd72c85fd5fe2913be520df32ed0
f4qgkb85q4pMRMChLeC7uSn2wwTWGXrs
09ce2f7bfb9243debf2c2efe05a1d047
308202ad30820216a00302010202044c26cea2300d06092a864886f70d010105050030819a310b3009060355040613023836311530130603550408130c4265696a696e6720436974793115301306035504071307c4265696a696e6720436974793126302406035504 [illegible] 5a6f6e652054656 [illegible] 63656e7420436f6d70616e793118301606035504 0b130f54656e63656e7420436f6d70616e79311b3019060355040313126 [illegible] 05465616d301e170d313030363237303430383032 5a170d333530363231303430383032 5a3081 [illegible] 3009060355040613023836311530130603550408130c4265696a696e6720436974793115301306035504071307c4265696a696e6720436974793126302406035504 0a131d5 [illegible] 54656e63656e7420436f6d70616e79311b3019060355040313126416e64726f696420515a6f6e652054656 16d30819f300d06092a864886f70d010101050003818d00308189028181 [illegible] 29e2a7fe02de99c27539602c026edf96ad8d43df32a85458bca1e6fbf11958658a7d [illegible] 1d9b782bf43a8c19bd [illegible] 580e340c46e6f306a772c1ef98f10a559edf867f3f31fe492808776b7bd953b2cba2d [illegible] 6003b04a8a8c5be9650f350cda6896e57dd13e6e83e7f891fc70f6a3c2eaf75c [illegible] 3cd19d95fbc1c2ac956309eda8eef3944baf08c4a49d3b9b3ffb06bc13da [illegible] 677
MCwwDQYJKoZIhvcNAQEBBQADGwAwGAIRAMRB/Q0hTCD+Xtn Qhp [illegible] CAwEAAQ==
7504f3f0-aca8-4636-b486-e396559d3efb

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。