南明离火
移动应用检测平台

ANDROID 静态分析报告

艾米直播 • v9.9.3

分析日期: 2025-04-03 10:18:15

应用概览

文件名称:	imifun_R9.9.3_64b.apk
文件大小:	84.88MB
应用名称:	艾米直播
软件包名:	com.mobimtech.natives.ivp
主活动:	com.mobimtech.natives.ivp.IvpSplashActivity
版本号:	9.9.3
最小SDK:	21
目标SDK:	30
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:	3/432
杀软检测:	AI评估：可能有安全隐患
MD5:	e809a6f3c3ea72f2d8648697af2792ac
SHA1:	4828bdc4f6b44243ec4f1fcd060995dcec0e611
SHA256:	8e00bf02f82a1a5[illegible]8b8621982100ebb0d[illegible]1e00f4c880f852b734be48b

分析结果严重性

高危	中危	信息	安全	关注
6	33	1	1	56

四大组件信息

Activity组件：118个，其中export的有： 10个
Service组件：17个，其中export的有： 6个
Receiver组件：10个，其中export的有： 4个
Provider组件：14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=086, ST=shanghai, L=shanghai, O=mobimtech, OU=mobimtech, CN=mobim
签名算法: rsassa_pkcs1v15
有效期自: 2013-09-25 07:42:01+00:00
有效期至: 2043-09-18 07:42:01+00:00
发行人: C=086, ST=shanghai, L=shanghai, O=mobimtech, OU=mobimtech, CN=mobim
序列号: 0x2cb172df
哈希算法: sha256
证书MD5: eda6523aa98f4cccc769dc32666e88b5
证书SHA1: 2bd45ef04c4650d93e932425a6df18fc2c3f6163
证书SHA256: aae920c80cd202b8e46c3784bcddad2c86ba2e6acae8e3a7821e56c8a6559454
证书SHA512:
c981e3cba0bf88b640aeec029cfa674516f401c80e282cb4f6d028e0eee72c6c121c9a8dc6db4e0116e8a2bf77391347c137bb109c79521d285fc8c5d5eff6e0

公钥算法: rsa
密钥长度: 2048
指纹: 29ba8e54452fd3df5586df920e319adf722e40d5073f6ff412b8d5cb1af42f0a
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.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。
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.READ_SETTINGS	危险	读取桌面快捷方式	这种权限的作用是允许应用读取桌面快捷方式的设置。
android.permission.DISABLE_KEYGUARD	危险	禁用键盘锁	允许应用程序停用键锁和任何关联的密码安全设置。例如，在手机上接听电话时停用键锁，在通话结束后重新启用键锁。
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.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.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.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.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.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_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.ACCESS_DOWNLOAD_MANAGER	签名(系统)	访问下载管理器	这个权限是允许应用访问下载管理器，以便管理大型下载操作。

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.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.hardware.sensor.accelerometer	未知	未知权限	来自 android 引用的未知权限。
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.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.FLASHLIGHT	普通	控制闪光灯	允许应用程序控制闪光灯。
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.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
com.mobimtech.natives.ivp.permission.MIPUSH_RECEIVE	未知	未知权限	来自 android 引用的未知权限。
com.mobimtech.natives.ivp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。
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.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。
com.mobimtech.natives.ivp.permission.RONG_ACCESS_RECEIVER	未知	未知权限	来自 android 引用的未知权限。
com.mobimtech.natives.ivp.permission.RONG_BRIDGE_ACTIVITY	未知	未知权限	来自 android 引用的未知权限。
com.mobimtech.natives.ivp.permission.PROCESS_PUSH_MSG	未知	未知权限	来自 android 引用的未知权限。
com.mobimtech.natives.ivp.permission.PUSH_PROVIDER	未知	未知权限	来自 android 引用的未知权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。
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
com.mobimtech.natives.ivp.IvpSplashActivity	Schemes: imi://,

com.tencent.tauth.AuthActivity	Schemes: tencent100397627://,
com.mobimtech.natives.ivp.common.pay.ThirdPartyWXPayActivity	Schemes: imih5pay://,

网络通信安全

高危: **2** | 警告: **0** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	imifun.com happyia.com mobimtech.com 119.28.28.98 119.29.29.98 43.132.55.55 43.134.43.43	高危	域配置不安全地配置为允许明文流量到达范围内的这些域。

证书安全分析

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分析

高危: **0** | 警告: **23** | 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=@xml/network_security_config]	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	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。
4	Activity (com.mobimtech.natives.ivp.wxapi.WXEntryActivity) 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。
5	Activity (com.tencent.tauth.AuthActivity) 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。

6	Activity (com.mobimtech.natives.ivp.mainpage.IvpMainActivity) 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。
7	Activity (com.mobimtech.natives.ivp.wxapi.WXPayEntryActivity) 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。
8	Broadcast Receiver (com.mobimtech.natives.ivp.push.receiver.MiReceiver) 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。
9	Service (com.mobimtech.natives.ivp.push.receiver.PushMessageService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.coloros.mcs.permission.SEND_MCS_MESSAGE [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。
10	Service (com.mobimtech.natives.ivp.push.receiver.AppPushMessageService) 受权限保护，但是应该检查权限的保护级别。 Permission: com.heytap.mcs.permission.SEND_PUSH_MESSAGE [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。
11	Service (com.vivo.push.sdk.service.CommandClientService) 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。
12	Broadcast Receiver (com.mobimtech.natives.ivp.push.receiver.ViVoPushMessageReceiverImpl) 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。
13	Service (com.xiaomi.mipush.sdk.PushMessageHandler) 受权限保护，但是应该检查权限的保护级别。 Permission: com.xiaomi.xmsf.permission.MIPUSH_RECEIVE [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。
14	Activity (com.xiaomi.mipush.sdk.NotificationClickedActivity) 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 (com.mobimtech.rongim.conversation.ConversationActivity) 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 (com.mobimtech.natives.ivp.common.pay.ThirdPartyWXPayActivity) 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。
17	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护, 但是应该检查权限的保护级别。 Permission: android.permission.DUMP [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。
18	Service (io.rong.push.rongpush.PushService) 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。
19	Broadcast Receiver (io.rong.push.rongpush.PushReceiver) 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。
20	Activity (io.rong.push.notification.RongBridgeActivity) 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。
21	Broadcast Receiver (com.huawei.hms.support.api.push.PushMsgReceiver) 受权限保护。 Permission: com.mobimtech.natives.ivp.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
22	Broadcast Receiver (com.huawei.hms.support.api.push.PushReceiver) 受权限保护。 Permission: com.mobimtech.natives.ivp.permission.PROCESS_PUSH_MSG protectionLevel: signature [android:exported=true]	信息	发现 Broadcast Receiver被导出，但受权限保护。
23	Service (com.huawei.hms.support.api.push.service.HmsMsgService) 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	Content Provider (com.huawei.hms.support.api.push.PushProvider) 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。
25	Activity (com.alipay.sdk.app.PayResultActivity) 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。
26	Activity (com.alipay.sdk.app.AlipayResultActivity) 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。

</> 安全漏洞检测

高危: **4** | 警告: **8** | 信息: **1** | 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
2	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
3	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
4	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
5	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

6	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
7	SSL的不安全实现。信任所有证书或接受自签名证书是一个关键的安全漏洞。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
8	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
9	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
10	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
11	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
12	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
13	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
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

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/libC2dxEngine.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。这使得动态返回的编程（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随机哨兵值，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

2	arm64-v8a/libobjectbox-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: ['__strlen_chk', '__memcpy_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk', '__vsprintf_chk']	True info 符号被剥离
3	arm64-v8a/libpine.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: ['__strlcat_chk', '__strcat_chk']	True info 符号被剥离

4	arm64-v8a/librongcloud_xcrash.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', '__strlen_chk', '__memcpy_chk']	True info 符号被剥离
5	arm64-v8a/librtslog.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', '__read_chk', '__strlen_chk']	True info 符号被剥离

6	arm64-v8a/libZegoExpressEngine.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', '__strlen_chk', '__memcpy_chk', '__memset_chk', '__strchr_chk', '__read_chk', '__vsnprintf_chk', '__memmove_chk']	True info 符号被剥离

行为分析

编号	行为	标签	文件
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
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
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
00162	创建 InetSocketAddress 对象并连接到它	socket	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
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
00013	读取文件并将其放入流中	文件	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

00209	从最新渲染图像中获取像素	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
00192	获取短信收件箱中的消息	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
00036	从 res/raw 目录获取资源文件	反射	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
00009	将游标中的数据放入JSON对象	文件	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
00056	修改语音音量	控制	升级会员：解锁高级权限
00028	从assets目录中读取文件	文件	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
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
00191	获取短信收件箱中的消息	短信	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
00043	计算WiFi信号强度	信息收集 WiFi	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

敏感权限分析

类型	匹配	权限
恶意软件常用权限	7/30	android.permission.CAMERA android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.WAKE_LOCK android.permission.SYSTEM_ALERT_WINDOW android.permission.REQUEST_INSTALL_PACKAGES

其它常用权限	14/46	com.android.launcher.permission.INSTALL_SHORTCUT android.permission.CHANGE_NETWORK_STATE android.permission.WRITE_EXTERNAL_STORAGE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH android.permission.CHANGE_WIFI_STATE android.permission.FLASHLIGHT android.permission.FOREGROUND_SERVICE android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_IMAGES android.permission.READ_MEDIA_VIDEO com.google.android.gms.permission.AD_ID

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
www.happyia.com	安全	是	**IP地址:** 139.199.10.145 **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
s1doll.imifun.com	安全	是	**IP地址:** 139.199.10.50 **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
im2.imifun.com	安全	否	No Geolocation information available.
proxy.mobimtech.com	安全	是	**IP地址:** 123.207.94.81 **国家:** 中国 **地区:** 广东 **城市:** 广州市 **纬度:** 23.1181 **经度:** 113.2539 **查看:** 高德地图
s1testmapi.imifun.com	安全	是	**IP地址:** 139.199.10.145 **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

ww4.sinaimg.cn	安全	是	**IP地址:** 139.199.10.145 **国家:** 中国 **地区:** 安徽 **城市:** 滁州 **纬度:** 32.321941 **经度:** 118.297783 **查看:** 高德地图
sysdk.cl2009.com	安全	是	**IP地址:** 139.199.10.145 **国家:** 中国 **地区:** l è x «IBwìBMôßwl è x «Û® éþAÉêBNôßwl è x «IBwìBOôßwl è x «Û®éþAÉêBPôßwl è x «IBwìBRôß **城市:** 上海 **纬度:** 31.224333 **经度:** 121.469948 **查看:** 高德地图
ww3.sinaimg.cn	安全	是	**IP地址:** 139.199.10.145 **国家:** 中国 **地区:** 安徽 **城市:** 滁州 **纬度:** 32.321941 **经度:** 118.297783 **查看:** 高德地图
s2proxy.imifun.com	安全	是	**IP地址:** 106.75.240.72 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
testmgetipv4.imifun.com	安全	是	**IP地址:** 139.199.68.219 **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
s2mapi.imifun.com	安全	是	**IP地址:** 111.230.226.180 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
sy.cl2m.cn	安全	是	**IP地址:** 106.14.53.48 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.2222 **经度:** 121.4581 **查看:** 高德地图

opt-sentry-prod.zego.cloud	安全	否	**IP地址:** 10.111.32.37 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图
opt-oms.zego.cloud	安全	否	**IP地址:** 10.1.75.82 **国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看:** Google 地图
s2doll.imifun.com	安全	是	**IP地址:** 111.230.226.163 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
wx.app100688440.twsapp.com	安全	是	**IP地址:** 123.207.130.132 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
console.happyia.com	安全	是	**IP地址:** 111.231.231.232 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
www.cmpassport.com	安全	是	**IP地址:** 112.33.110.15 **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
wx.mobimtech.com	安全	是	**IP地址:** 139.199.2.137 **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
loot.mobimtech.com	安全	是	**IP地址:** 139.199.68.219 **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

test-weixin.imifun.com	安全	是	**IP地址:** 139.199.2.137 **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
loot.imifun.com	安全	是	**IP地址:** 111.231.231.62 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
lame.sf.net	安全	否	**IP地址:** 104.18.31.237 **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
s2zhuanpan.imifun.com	安全	是	**IP地址:** 111.230.155.198 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
mobileapi.mobimtech.com	安全	是	**IP地址:** 139.199.2.137 **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
rim.mobimtech.com	安全	是	**IP地址:** 111.230.245.224 **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
aimi.mobimtech.com	安全	是	**IP地址:** 111.230.245.224 **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
ivpim.imifun.com	安全	是	**IP地址:** 111.230.245.224 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图

mini.imifun.com	安全	是	**IP地址:** 111.230.245.224 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
cdnfile.imifun.com	安全	是	**IP地址:** 111.230.245.224 **国家:** 中国 **地区:** 陕西 **城市:** 咸阳 **纬度:** 34.337780 **经度:** 108.702606 **查看:** 高德地图
upload-bbs.miyoushe.com	安全	是	**IP地址:** 42.222.46.202 **国家:** 中国 **地区:** 江苏 **城市:** 宿州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
mgetipv4.imifun.com	安全	是	**IP地址:** 175.178.248.254 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
im.imifun.com	安全	否	No Geolocation information available.
s2.imifun.com	安全	是	**IP地址:** 106.55.240.72 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
zhuanpan.imifun.com	安全	是	**IP地址:** 111.231.231.62 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
s2loot.imifun.com	安全	是	**IP地址:** 111.230.155.198 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图

objectbox.io	安全	否	**IP地址:** 85.13.163.69 **国家:** 德国 **地区:** 图林根 **城市:** 弗里德斯多夫 **纬度:** 50.604919 **经度:** 11.035770 **查看:** Google 地图
auth.wosms.cn	安全	是	**IP地址:** 124.64.196.35 **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
qn-static.imifun.com	安全	是	**IP地址:** 180.97.228.162 **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
minitest.imifun.com	安全	是	**IP地址:** 139.199.68.32 **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
ww2.sinaimg.cn	安全	是	**IP地址:** 223.244.13.80 **国家:** 中国 **地区:** 安徽 **城市:** 滁州 **纬度:** 32.321941 **经度:** 118.297783 **查看:** 高德地图
s1mapi.imifun.com	安全	是	**IP地址:** 111.230.245.224 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
s2wx.imifun.com	安全	是	**IP地址:** 111.230.155.198 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
static.mobpmtech.com	安全	是	**IP地址:** 139.199.5.237 **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

wap.cmpassport.com	安全	是	**IP地址:** 120.232.169.168 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
wx.app100690641.twsapp.com	安全	是	**IP地址:** 111.231.231.62 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
fruit9009.imifun.com	安全	是	**IP地址:** 106.52.70.252 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
zhuanpan.mobimtech.com	安全	是	**IP地址:** 139.199.68.219 **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
fs.cl2009.com	安全	是	**IP地址:** 47.101.5.82 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
static.happyia.com	安全	是	**IP地址:** 180.97.228.82 **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
ww1.sinaimg.cn	安全	是	**IP地址:** 223.244.13.63 **国家:** 中国 **地区:** 安徽 **城市:** 滁州 **纬度:** 32.321941 **经度:** 118.297783 **查看:** 高德地图
ivpim.mobimtech.com	安全	是	**IP地址:** 118.89.16.156 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图

s1proxy.imifun.com	安全	是	**IP地址:** 111.231.231.62 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
fruit9009.mobimtech.com	安全	是	**IP地址:** 139.199.68.219 **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
s1wx.imifun.com	安全	是	**IP地址:** 139.199.68.219 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
s2fruit9009.imifun.com	安全	是	**IP地址:** 139.199.68.219 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
m.imifun.com	安全	是	**IP地址:** 111.231.231.146 **国家:** 中国 **地区:** 广东 **城市:** 广州 **纬度:** 23.127361 **经度:** 113.264572 **查看:** 高德地图
cdn.mobimtech.com	安全	是	**IP地址:** 139.199.5.237 **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
e.189.cn	安全	是	**IP地址:** 42.123.76.65 **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
docs.zegocloud.com	安全	是	**IP地址:** 47.242.198.129 **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

app100690641.imgcache.qzoneapp.com	安全	是	**IP地址:** 116.55.250.66 **国家:** 中国 **地区:** 云南 **城市:** 昆明 **纬度:** 25.038891 **经度:** 102.718330 **查看:** 高德地图
static.imifun.com	安全	是	**IP地址:** 223.247.117.235 **国家:** 中国 **地区:** 安徽 **城市:** 亳州 **纬度:** 33.877220 **经度:** 115.770279 **查看:** 高德地图
doll.mobimtech.com	安全	是	**IP地址:** 139.199.68.32 **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
cdnstatic.imifun.com	安全	是	**IP地址:** 223.247.117.235 **国家:** 中国 **地区:** 安徽 **城市:** 亳州 **纬度:** 33.877220 **经度:** 115.770279 **查看:** 高德地图

URL链接分析

URL信息	源码文件
• https://turing.captcha.qcloud.com/TCaptcha.js • https://auth.wosms.cn • https://ms.zzx9.cn • https://daily.m.zzx9.cn • https://m.zzx.cnklog.com • https://msv6.wosms.cn	自研引擎-A
• https://cdnstatic.imifun.com/ivp/images/game_mobile/lucky_new_2018/freqtable.png	com/mobimtech/natives/ivp/game/roller/RollerProbDialogFragment.java
• file:///assets/	com/opensource/svgaplayer/SVGAParser$decodeFromAssets$1.java
• 2.3.6.4	com/chuanglan/shanyan_sdk/tool/c.java
• www.cmpassport.com	com/chuanglan/shanyan_sdk/utils/q.java
• 224.0.0.1 • 255.255.255.255 • 127.0.0.1	com/chuanglan/shanyan_sdk/utils/p.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/IterableKt.java

• https://github.com/arrow-kt/arrow/issues	arrow/core/IorKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/MapKt.java
• http://app100690641.imgcache.qzoneapp.com/app100690641/flash/app/ivp_video_1.0.58_v6245.swf	com/SimpleRtmp/rtmp/io/FmsConnection.java
• http://m.imifun.com	com/mobimtech/natives/ivp/common/util/ShareUtils.java
• https://github.com/yyued/svgaplayer-android#cache	com/opensource/svgaplayer/download/FileDownloader$resume$2.java
• https://static.mobimtech.com/ivp/	com/mobimtech/natives/ivp/specialeffect/SpecialEffectRemotePathKt.java
• 2.3.6.4 • https://fs.cl2009.com/flash/thin/accountinit/v3	com/chuanglan/shanyan_sdk/tool/l.java
• 119.28.28.99 • 119.29.29.98 • 119.28.28.98 • 119.29.29.99	a/a/a/a/a.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/ResultKt.java
• 2.3.6.4	com/chuanglan/shanyan_sdk/tool/k.java
• https://github.com/kizitonwose/calendar/blob/3dfb2d2e91d5e443b540f41113a05268e4b8d2/sample/src/main/java/com/kizitonwose/calendar/sample/view/example6Fragment.kt#l29	com/kizitonwose/calendar/view/internal/ItemRootKt.java
• 2.3.6.4	com/chuanglan/shanyan_sdk/e/g.java

• http://static.happyia.com/ivp/roombanner/dailytask6.png • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384305780.png • www.happyia.com • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384312308.png • http://static.mobimtech.com/ivp//avatar/avatar/2016/11/14/1479110249773_mobile_live.jpg • http://ww1.sinaimg.cn/large/7a8aed7bgw1etkpwkaxqej20gy0pfta8.jpg • http://static.happyia.com/ivp/roombanner/dailytask14.png • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384292983.png • http://static.mobimtech.com/ivp//avatar/avatar/2019/6/21/1561080470776_scale151.jpg • http://wx.app100690641.twsapp.com/act-10085.jsp • http://ww4.sinaimg.cn/large/7a8aed7bjw1f0f9fkzu78j20f00qo0xl.jpg • http://static.happyia.com/ivp//avatar/avatar/2015/1/5/1420444845657_scale151.jpg • http://ww1.sinaimg.cn/large/7a8aed7bgw1ettzpowndgj216g0s4dkg.jpg • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384324955.png • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384318784.png • http://static.mobimtech.com/ivp//console/images/activity/1390542767293.png • http://static.mobimtech.com/ivp//avatar/avatar/2019/6/3/1559551319640p_final.jpg • http://a/b/c/d/ • http://static.happyia.com/ivp//avatar/avatar/2016/12/28/1482911300974_scale151.jpg • http://static.happyia.com/ivp/spirit/3.png • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384331539.png • http://ww4.sinaimg.cn/large/7a8aed7bjw1f14fbwrfptj20zk0npgtu.jpg • http://wx.app100690641.twsapp.com/activity/annualfestivalrank2017?flag=1 • http://static.happyia.com/ivp//avatar/avatar/2016/6/7/1465277267279_scale151.jpg • http://ww2.sinaimg.cn/large/7a8aed7bgw1exmhnx76z9j20go0dcabp.jpg • http://static.mobimtech.com/ivp//avatar/avatar/2016/12/21/1482287801872_scale151.jpg • http://static.happyia.com/ivp//avatar/avatar/2015/12/22/1450764922111_scale151.jpg • http://static.happyia.com/ivp/spirit/4.png • http://static.mobimtech.com/ivp//avatar/avatar/2019/6/3/1559551334869_new_mobile_live.jpg • http://ww1.sinaimg.cn/large/7a8aed7bjw1exe9ssy2gsj20qo0hndjr.jpg • http://wx.app100688440.twsapp.com/activity/spring • http://static.mobimtech.com/ivp/avatar/avatar/2019/10/16/1571221604495_final.jpg • http://wx.mobimtech.com/bigcustomer • http://static.happyia.com/ivp/spirit/1.png • http://ww4.sinaimg.cn/large/610dc034jw1faoucp1idej20u011h0va.jpg • http://static.happyia.com/ivp/roombanner/dailytask12.png • http://static.mobimtech.com/ivp//avatar/avatar/2015/1/20/1421738217756p_final.jpg • http://static.mobimtech.com/ivp/avatar/avatar/2015/1/5/1420435432113_final.jpg • http://static.happyia.com/ivp//avatar/avatar/2017/7/18/1500348180544_scale151.jpg • http://static.happyia.com/ivp//avatar/avatar/2016/6/7/1465277211664_scale151.jpg • http://static.happyia.com/ivp/roombanner/dailytask5.png • http://ww3.sinaimg.cn/large/7a8aed7bgw1ewy3cst6rzj20lx0y4wj5.jpg • http://static.happyia.com/ivp/roombanner/dailytask11.png • http://static.happyia.com/ivp/spirit/2.png • http://console.happyia.com:8091/main/appmanager/mobilebanner?moduleid=152 • https://cdnstatic.imifun.com/ivp//activitytemplate/taskpanel/1503384299517.png • http://ww2.sinaimg.cn/large/610dc034gw1farbzilkcj20u00u076w.jpg • http://static.happyia.com/ivp/roombanner/dailytask13.png • http://static.happyia.com/ivp/roombanner/dailytask15.png • http://ww4.sinaimg.cn/large/7a8aed7bgw1esvx1z5iu6j20hs0qo428.jpg	com/mobimtech/natives/ivp/common/http/MockResponseInfoFactory.java
• https://objectbox.io/sync/	io/objectbox/sync/server/SyncServerBuilder.java
• 2.3.6.4	com/chuanglan/shanyan_sdk/d/f.java
• https://testmgetipv4.imifun.com/ • https://mgetipv4.imifun.com/	com/mobimtech/ivp/login/IPConfigUseCase.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/Ior.java
• 119.29.29.98	com/mobimtech/natives/ivp/common/util/ProtocolUtils.java
• https://cdnstatic.imifun.com/ivp/pic/global_badge/1679290128188.png • https://cdnstatic.imifun.com/ivp/pic/global_badge/1711072149557.png • http://static.mobimtech.com/ivp/pic/global_badge/1528178324130.png • http://static.mobimtech.com/ivp/pic/global_badge/1553046859619.png • http://static.mobimtech.com/ivp/pic/global_badge/1528766682058.png • http://static.mobimtech.com/ivp/pic/global_badge/1615363033930.png	com/mobimtech/ivp/core/api/fake/FakeRoomDataSource.java
• http://mobileapi.mobimtech.com/uploadservlet • http://mobileapi.mobimtech.com/app/open/open.do?acid=1003&uid=104718 • http://static.mobimtech.com/ivp//avatar/avatar/2024/1/11/1704951146741_final.png	com/mobimtech/ivp/core/api/fake/FakeLoginDataSource.java

本报告由南明离火移动安全分析平台生成

• https://github.com/arrow-kt/arrow-core/issues/new/choose	arrow/core/ArrowCoreInternalException.java
• http://static.mobimtech.com/ivp/spirit/3.png • https://cdnstatic.imifun.com/ivp/mobile_activity/loot-introduce/index.html • http://static.mobimtech.com/ivp/spirit/5.png • http://static.mobimtech.com/ivp/spirit/1.png • http://static.mobimtech.com/ivp/spirit/2.png	com/mobimtech/ivp/core/api/fake/FakeMission.java
• http://static.mobimtech.com/ivp/ivp/images/achievement/010101.png • https://upload-bbs.miyoushe.com/upload/2024/04/17/2393822/2de403d599087593f7149ae22d7fe342_2640169551745216641.jpg?x-oss-process=image/resize,s_600/quality,q_80/auto-orient,0/interlace,1/format,jpg	com/mobimtech/ivp/core/api/fake/FakeHomeWebSocketMessage.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/ConstKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/ValidatedKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/Validated.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/SequenceKt.java
• https://objectbox.io/sync/	io/objectbox/sync/SyncBuilder.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/TupleNKt.java
• 2.3.6.4	com/chuanglan/shanyan_sdk/tool/i.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/EitherKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/Either.java
• https://github.com/kizitonwose/calendar/blob/3dfb2d2e01d5e443b540ff411113a05268e4b8d2/sample/src/main/java/com/kizitonwose/calendar/sample/view/example6fragment.kt#l29	com/kizitonwose/calendar/view/internal/yearcalendar/YearRootKt.java
• https://sy.cl2m.cn/flash/accountinit/v4 • https://sysdk.cl2009.com • https://sy.cl2m.cn • https://sy.cl2m.cn/flash/thin/accountinit/v3 • https://sysdk.cl2009.com/log/fdr/v3	com/chuanglan/shanyan_sdk/a/e.java
• https://auth.wosms.cn/html/oauth/protocol2.html • 2.3.6.4 • https://wap.cmpassport.com/resources/html/contract.html • https://e.189.cn/sdk/agreement/detail.do?hidetop=true	com/chuanglan/shanyan_sdk/a/a.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/NonEmptyListKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/typeclasses/Semigroup.java
• https://s2wx.imifun.com/ • https://cdnfile.imifun.com/www/ivp/ • http://im2.imifun.com/ • https://qn-static.imifun.com/ivp/ • https://s2loot.imifun.com/ • https://s2fruit9009.imifun.com/ • https://s2mapi.imifun.com/app/ • https://s2doll.imifun.com • https://s2zhuanpan.imifun.com/ • https://s2.imifun.com/ • https://s2proxy.imifun.com/	com/mobimtech/natives/ivp/common/http/protocol/Zone2DefaultUrl.java

• wss://ivpim.imifun.com/ • https://cdnfile.imifun.com/www/ivp/ • https://im.imifun.com/ • https://zhuanpan.imifun.com/ • https://qn-static.imifun.com/ivp/ • https://loot.imifun.com/ • https://fruit9009.imifun.com/ • https://s1wx.imifun.com/ • https://s1proxy.imifun.com/ • https://s1doll.imifun.com/ • https://aimi.mobimtech.com/ • https://s1mapi.imifun.com/app/	com/mobimtech/natives/ivp/common/http/protocol/Zone1DefaultUrl.java
• https://mini.imifun.com/ • http://static.imifun.com/m_down.html • https://minitest.imifun.com/ • https://wpa1.qq.com/yxmjucfn?_type=wpa&qidian=true	com/mobimtech/natives/ivp/common/http/protocol/UrlHelper.java
• https://github.com/kizitonwose/calendar/blob/3dfb2d2e91d5e443b540ff411113a05268e4b0ad/sample/src/main/java/com/kizitonwose/calendar/sample/view/example6fragment.kt#l29	com/kizitonwose/calendar/view/internal/CustomViewClassKt.java
• https://%s/d?%s	a/a/a/a/d/p/c/a.java
• http://%s/d?%s&alg=des	a/a/a/a/d/p/b/b.java
• https://github.com/arrow-kt/arrow/issues	x2/b.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/OptionKt.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/Option.java
• 2.3.6.4 • https://sy.cl2m.cn • https://sysdk.cl2009.com	com/chuanglan/shanyan_sdk/a.java
• http://%s/d?%s&alg=aes	a/a/a/a/d/p/a/b.java
• http://cdn.mobimtech.com/www/ivp/ • https://rim.mobimtech.com/ • http://zhuanpan.mobimtech.com/ • https://cdnstatic.imifun.com/ivp/ • wss://ivpim.mobimtech.com/ • http://proxy.mobimtech.com/ • http://aimi.mobimtech.com/ • https://test-wei.in.imifun.com/ • http://doll.mobimtech.com:8080 • https://s1testmapi.imifun.com/app/ • http://fruit9009.mobimtech.com/ • http://loot.mobimtech.com/	com/mobimtech/natives/ivp/common/http/protocol/TestDefaultUrl.java
• https://github.com/zieiony/carbon/issues	carbon/Carbon.java
• https://static.imifun.com/privacy/auth-camera.html • https://static.imifun.com/privacy/auth-storage.html • https://static.imifun.com/privacy/auth-record.html	com/mobimtech/natives/ivp/setting/PrivacySettingActivity.java
• https://github.com/arrow-kt/arrow/issues	arrow/core/TupleNKt__PairKt.java

• http://static.imifun.com/ivp/flash/ivp_video_1.0.10_v5159.swf?v2	com/SimpleRtmp/rtmp/io/ChatConnection.java
• https://www.baidu.com/img/bd_logo1.png	com/mobimtech/natives/ivp/mainpage/avatar/MockAnimatedAvatarRepository.java
• https://static.imifun.com/privacy/amzb-privacy.html • https://static.imifun.com/privacy/amzb-privacy.html#3rdpri • https://static.imifun.com/privacy/users_imizb.html	自研引擎-S
• 1.2.0.4 • ftp://%s:%s@%s	lib/arm64-v8a/libC2dkEngine.so
• https://objectbox.io/sync/	lib/arm64-v8a/libobjectbox-jni.so
• https://github.com/canyie/pine/issues/8	lib/arm64-v8a/libpine.so
• http://d9473d8f56814fdbde0813c5a7ca4fe0@opt-sentry-prod.zego.cloud/5 • 127.0.0.1 • http://38598faa2bd5ac6f5c5dfcec7b4a7fa4@opt-sentry-prod.zego.cloud/9 • http://opt-oms.zego.cloud/#/log-server/sdk-log/info? • file://localfile • 1.4.0.52 • 1.2.0.4 • https://docs.zegocloud.com/article/5547 • 8.8.8.8 • http://lame.sf.net	lib/arm64-v8a/libZegoExpressEngine.so

第三方SDK

SDK名称	开发者	描述信息
MSA SDK	移动安全联盟	移动智能终端补充设备标识体系统一调用 SDK 由中国信息通信研究院泰尔终端实验室、移动安全联盟联合提供，知识产权归中国信息通信研究院所有。
C++ 共享库	Android	在 Android 应用中运行原生代码。
岳鹰全景监控	Alibaba	岳鹰全景监控是阿里 UC 官方出品的先进移动应用线上监控平台，为多家知名企业提供服务。
极光认证 SDK	极光	极光认证整合了三大运营商的网关认证能力，为开发者提供了一键登录和号码认证功能，优化用户注册/登录、号码验证的体验，提高安全性。
Jetpack DataStore	Google	Jetpack DataStore 是一种数据存储解决方案，允许您使用协议缓冲区存储键值对或类型化对象。DataStore 使用 Kotlin 协程和 Flow 以异步、一致的事务方式存储数据。
腾讯云 HTTPDNS	Tencent	HTTPDNS 基于 HTTP 协议向腾讯云的 DNS 服务器发送域名解析请求，替代了基于 DNS 协议向运营商 LocalDNS 发起解析请求的传统方式，可以避免 LocalDNS 造成的域名劫持和跨网访问问题，解决移动互联网服务中域名解析异常带来的困扰。
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。
android-gif-drawable	koral--	android-gif-drawable 是在 Android 上显示动画 GIF 的绘制库。
融云 IM SDK	融云 RongCloud	IM 即时通讯 - SealTalk 支持应用内社交等场景，体验单群聊、聊天室、音视频通话、小视频、动态表情等通讯能力

RenderScript	Android	RenderScript 是用于在 Android 上以高性能运行计算密集型任务的框架。RenderScript 主要用于数据并行计算，不过串行工作负载也可以从中受益。RenderScript 运行时可在设备上提供的多个处理器（如多核 CPU 和 GPU）间并行调度工作。这样您就能够专注于表达算法而不是调度工作。RenderScript 对于执行图像处理、计算摄影或计算机视觉的应用来说尤其有用。
闪验 SDK	创蓝云智	闪验整合三大运营商，支持国内三网手机号段，Android/iOS 手机，可通过一键获取用户手机号的 SDK 产品，建立以手机号码作为去中心化的开放账号体系，提升注册转换效率的必备功能。
SQLite	SQLite	SQLite 是遵守 ACID 的关系数据库管理系统，它包含在一个相对小的 C 程序库中。与许多其它数据库管理系统不同， SQLite 不是一个客户端/服务器结构的数据库引擎，而是被集成在用户程序中。 SQLite 遵守 ACID ， 实现了大多数 SQL 标准。它使用动态的、弱类型的 SQL 语法。
移动统计分析	Umeng	U-App 作为一款专业、免费的移动统计分析产品。在日常业务中帮您解决多种数据相关问题，如数据采集与管理、业务监测、用户行为分析、App 稳定性监控及实现多种运营方案等。助力互联网企业充分挖掘用户行为数据价值，找到产品更新迭代方向，实现精细化运营，全面提升业务增长效能。
即构极速视频 SDK	即构	极速视频（Express Video）是一款实时的音视频互动服务产品，能够为开发者提供便捷接入、高可靠、多平台互通的音视频服务。通过低至 200 ms 的端到端平均时延，业内领先的保障弱网质量的 QoS 策略，并结合强大的 3A 处理能力，完美支持一对多、多对多的实时音视频通话、直播、会议等场景。
支付宝 SDK	Alipay	支付宝开放平台基于支付宝海量用户，将强大的支付、营销、数据能力，通过接口等形式开放给第三方合作伙伴，帮助第三方合作伙伴创建更具竞争力的应用。
移动号码认证	中国移动	号码认证能力提供一键登录、本机号码校验服务。
HMS Core	Huawei	HMS Core 是华为终端云服务提供的端、云开放能力的合集，助您高效构建精品应用。
Huawei Push	Huawei	华为推送服务（HUAWEI Push Kit）是华为为开发者提供的消息推送平台，建立了从云端到终端的消息推送通道。开发者通过集成 HUAWEI Push Kit 可以实时推送消息到用户终端应用，构筑良好的用户关系，提升用户的感知度和活跃度。
PictureSelector	LuckSiege	一款针对 Android 平台下的图片选择器，支持从相册获取图片、视频、音频 & 拍照，支持裁剪(单图or 多图裁剪)、压缩、主题自定义配置等功能，支持动态获取权限&适配 Android 5.0+ 系统的开源图片选择框架
腾讯开放平台	Tencent	腾讯核心内部服务，二十年技术沉淀，助你成就更高梦想。
vivo Push	vivo	vivo 推送是 Funtouch OS 上系统级消息推送平台，帮助开发者在 vivo 平台有效提升活跃和留存。通过和系统的深度结合，建立稳定可靠、安全可控、高性能的消息推送服务，帮助不同行业的开发者挖掘更多的运营价值。
MiPush	Xiaomi	小米消息推送服务在 MIUI 上为系统级通道，并且全平台通用，可以为开发者提供稳定、可靠、高效的推送服务。
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。
AppGallery Connect	Huawei	为开发者提供移动应用全生命周期服务，覆盖全终端全场景，降低开发成本，提升运营效率，助力商业成功。
HMS Core AAID	Huawei	华为推送服务开放能力合集提供的匿名设备标识(AAID) 实体类与令牌实体类包。异步方式获取的 AAID 与令牌通过此包中对应的类承载返回。
OkDownload	LingoChamp	可靠，灵活，高性能以及强大的下载引擎。
Jetpack Media	Google	与其他应用共享媒体内容和控件。已被 media2 取代。

Jetpack ProfileInstaller	[Google](#)	让库能够提前预填充要由 ART 读取的编译轨迹。
Jetpack AppCompat	[Google](#)	Allows access to new APIs on older API versions of the platform (many using Material Design).
Jetpack Room	[Google](#)	Room 持久性库在 SQLite 的基础上提供了一个抽象层，让用户能够在充分利用 SQLite 的强大功能的同时，获享更强健的数据库访问机制。
OPPO Push	[OPPO](#)	OPPO PUSH 是 ColorOS 上的系统级通道，为开发者提供稳定，高效的消息推送服务。

邮箱

EMAIL	源码文件
38598faa2bd5ac6f5c5dfcec7b4a7fa4@opt-sentry-prod.zego.cloud d9473d8f56814fdbde0813c5a7ca4fe0@opt-sentry-prod.zego.cloud	lib/arm64-v8a/libZegoExpressEngine.so

追踪器

名称	类别	网址
Huawei Mobile Services (HMS) Core	Location, Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Yueying Crash SDK	Analytics, Crash reporting	https://reports.exodus-privacy.eu.org/trackers/448

密钥凭证

可能的密钥
vivo推送的=> "local_iv" : "MzMsMzQsMzUsMzYsMzcsMzgsMzksNDAsNDEsMzIsMzgsMzcsMzYsMzUsMzQsMzMsI0AzNCwzMiwzMywzNywzMywzNCwzMiwzMywzMywzMywzNCw0MSwzNSwzNSwzMiwzMiwjQDMzLDM0LDM1LDM2LDM3LDM4LDM5LDQwLDQxLDMyLDM4LDM3LDMzLDM1LDM0LDMzLCNAMzQsMzIsMzMsMzcsMzMsMzQsMzIsMzMsMzMsMzMsMzQsNDEsMzUsMzIsMzIsMzI"
华为HMS Core 应用ID的=> "com.huawei.hms.client.appid" : "appid=10100536"
vivo推送的=> "com.vivo.push.api_key" : "1dfb7f8e-e789-47cf-846e-53ba3cbf0b07"
友盟统计的=> "UMENG_APPKEY" : "523fd0cc56240b084f0711f7"
vivo推送的=> "com.vivo.push.app_id" : "13512"
友盟统计的=> "UMENG_MESSAGE_SECRET" : "8f4fe21f3c28a5cbf41c9ad3a3415a63"
29635bc7d3fe730f923eec2b71b8468e
20191017142016585293
10024-1-c96601649a5a8ba0d132f15f7c9230c5
103573-1-ac5142183d2d82b6c1f3c4634dd03fb9

本报告由南明离火移动安全分析平台生成

20170104174957323836
104416-1-8bd166252479e0a4c6170a078a7fde5c
12081114D8F2285f02edb7c582977180
6acb9422e34208d1cde7728f3a878101
CFAB183CA4569BC11886BEECE38CF63A
101161-1-c13671d12f7af8bab764088d06034213
154d6d758aec5e91b520fe4d21b5aae0
8cf23e49079f0b19fa6a9d1ddfb8b6cd
20170824165904636999
20170629170838364002
20170828145850669946
100-1-86171fca3c182f44d97e16d1c28c62b2
3dfb2d2e91d5e443b540ff411113a05268e4b8d2
105004-1-e29f045ab99d68472c31413b8a4efc27
103831-1-95984365d21b01e1760e57ba9b713382
9009-14-dc91ebdf465a8b3f92f836dbe153bce7
adaddcffe4bfd578b8cb667d08227d3d
2de403d599087593f7149ae22d7fe342
105180-1-48d01fe875731cf34907b36c21a90b4f

免责声明及风险提示: