南明离火
移动应用检测平台

ANDROID 静态分析报告

050 IP Phone: v2.3.0

分析日期: 2025-08-04 11:08:36

应用概览

文件名称:	050 IP Phone v2.3.0.apk
文件大小:	23.77MB
应用名称:	050 IP Phone
软件包名:	com.ntt.voip.android.sdk050voip
主活动:	com.ntt.voip.android.sdk050voip.client.ConfirmPermissionActivity
版本号:	2.3.0
最小SDK:	28
目标SDK:	34
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	48/100 (中风险)
跟踪器检测:	2/432
杀软检测:	经检测，该文件安全
MD5:	2d7a93f1ab90d90cc0ba6d17defe5b6d
SHA1:	231ca26986dd92eb8b14a96d68ff1d7f55d92ca1
SHA256:	0fd9b3f80bf9a162b1a2d50c46b3a1d854435faebd7b57b4f3c15a95fe1b57eff

分析结果严重性分布

高危	中危	信息	安全	关注
4	27	3	2	1

四大组件导出状态统计

Activity组件：54个，其中export的有： 4个
Service组件：19个，其中export的有： 2个
Receiver组件：20个，其中export的有： 6个
Provider组件：5个，其中export的有： 0个

应用签名证书信息

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
v4 签名: False
主题: C=JP, ST=Tokyo, L=Chiyoda-ku, O=NTT Communications Corporation, OU=Business Network Services Division, CN=NTT Communications Corporation
签名算法: rsassa_pkcs1v15
有效期自: 2010-12-03 01:10:56+00:00
有效期至: 2038-04-20 01:10:56+00:00
发行人: C=JP, ST=Tokyo, L=Chiyoda-ku, O=NTT Communications Corporation, OU=Business Network Services Division, CN=NTT Communications Corporation
序列号: 0x4cf843a0
哈希算法: sha1
证书MD5: b659067c87fd669daffbf7f4a1d94194
证书SHA1: d78d4172c1a6d652e414e2bca5da026b164a60d2
证书SHA256: 3ffb9fcde866057e9065fa6a14841dd017156126db2249ee23c50c4ada28abd1
证书SHA512: b1e4f7bad52b1010cff50d1cc4565344387f934e5e129117f9847d4def8c3344dc45d1be06[illegible]206c306b0833e00a4427[illegible]4121c983a752c0e5e4826a25cdc57f

公钥算法: rsa
密钥长度: 1024
指纹: e60cc5bb52fd584d30b499a239aa9cd4229b0cbb1788b39a812e037[illegible]bfc50[illegible]8
共检测到 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.ntt.voip.android.sdk050voip.permission.C2D_MESSAGE	未知	未知权限	来自 android 引用的未知权限。
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.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.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.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.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.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.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.BLUETOOTH_CONNECT	危险	新蓝牙运行时权限	Android 12 系统引入了新的运行时权限，需要能够连接到配对的蓝牙设备。
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。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	普通	使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS 的权限	应用程序必须拥有权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.SCHEDULE_EXACT_ALARM	普通	精确的闹钟权限	允许应用程序使用准确的警报 API。
android.permission.USE_FULL_SCREEN_INTENT	普通	全屏通知	Android 10以后的全屏 Intent 的通知
android.permission.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.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。
android.permission.FOREGROUND_SERVICE_MICROPHONE	普通	允许使用麦克风的前台服务	允许常规应用程序使用类型为“麦克风”的 Service.startForeground。
android.permission.READ_CONTACTS	危险	读取联系人信息	允允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可借此将您的数据发送给其他人。
android.permission.WRITE_CONTACTS	危险	写入联系人信息	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可借此清除或修改您的联系人数据。
android.permission.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_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_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。
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_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.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_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.PROCESS_OUTGOING_CALLS	危险	拦截外拨电话	允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
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.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_BACKGROUND_LOCATION	危险	获取后台定位权限	允许应用程序访问后台位置。如果您正在请求此权限，则还必须请求ACCESS COARSE LOCATION或ACCESS FINE LOCATION。单独请求此权限不会授予您位置访问权限。
android.permission.FOREGROUND_SERVICE_LOCATION	普通	允许前台服务与位置使用	允许常规应用程序使用类型为“location”的 Service.startForeground。
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.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
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。
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	普通	允许应用程序访问广告服务归因	这使应用能够检索与广告归因相关的信息，这些信息可用于有针对性的广告目的。应用程序可以收集有关用户如何与广告互动的数据，例如点击或展示，以衡量广告活动的有效性。
android.permission.ACCESS_ADSERVICES_AD_ID	普通	允许应用访问设备的广告 ID。	此 ID 是 Google 广告服务提供的唯一、用户可重置的标识符，允许应用出于广告目的跟踪用户行为，同时维护用户隐私。
com.ntt.voip.android.sdk050voip.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	未知权限	来自 android 引用的未知权限。

可浏览 Activity 组件分析

ACTIVITY	INTENT
com.ntt.voip.android.com050plus.client.MainActivityFromUri	Schemes: tel://,
com.ntt.voip.android.com050plus.client.MainActivityFromCom050Uri	Schemes: sdk050voip://, Hosts: keypad, initsetpfb,

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	应用已使用代码签名证书进行签名。

Manifest 配置安全分析

高危: **1** | 警告: **16** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息
1	应用已配置网络安全策略 [android:networkSecurityConfig=@7F150001]	信息	网络安全配置允许应用通过声明式配置文件自定义网络安全策略，无需修改代码。可针对特定域名或应用范围进行灵活配置。
2	Broadcast Receiver (com.ntt.voip.android.com050plus.client.outgoing.OutgoingCallReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
3	Service (com.ntt.voip.android.com050plus.client.outgoing.SdkCallRedirectionService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_CALL_REDIRECTION_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
4	Activity 设置了 TaskAffinity 属性 (com.ntt.voip.android.com050plus.client.MainActivityFromPhone)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
5	Activity （com.ntt.voip.android.com050plus.client.MainActivityFromPhone）如果未对输入进行校验，此配置允许同一设备上没有任何权限的第三方应用程序调用它并发起电话呼叫，而无需用户交互。	高危	一个导出的Activity ，如果没有对接收Intent的输入验证，则可以调用拨号程序进行拨打电话而无需用户交互，这很可能是一个高危漏洞，请人工核验。 参考：CVE-2024-37574
6	Activity (com.ntt.voip.android.com050plus.client.MainActivityFromPhone) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
7	Activity 设置了 TaskAffinity 属性 (com.ntt.voip.android.com050plus.client.MainActivityFromUri)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
8	Activity (com.ntt.voip.android.com050plus.client.MainActivityFromUri) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。

9	Activity-Alias (com.ntt.voip.android.com050plus.client.MainActivityFromCom050Uri) 未受保护。 [android:exported=true]	警告	检测到 Activity-Alias 已导出，未受任何权限保护，任意应用均可访问。
10	Activity (com.oki_access.android.ims.call.client.SearchContactListActivity) 未受保护。 [android:exported=true]	警告	检测到 Activity 已导出，未受任何权限保护，任意应用均可访问。
11	Activity 设置了 TaskAffinity 属性 (com.oki_access.android.ims.call.client.TurnScreenOnActivity)	警告	设置 taskAffinity 后，其他应用可读取发送至该 Activity 的 Intent。为防止敏感信息泄露，建议保持默认 affinity（包名）。
12	Broadcast Receiver (com.ntt.voip.android.service.ImsServiceStarter) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
13	Broadcast Receiver (com.ntt.voip.android.extension.control.MediaActionReceiver) 未受保护。 [android:exported=true]	警告	检测到 Broadcast Receiver 已导出，未受任何权限保护，任意应用均可访问。
14	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) 受权限保护，但应检查权限保护级别。 Permission: com.google.android.c2dm.permission.SEND [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
15	Service (androidx.work.impl.background.systemjob.SystemJobService) 受权限保护，但应检查权限保护级别。 Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	警告	检测到 Service 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
16	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。

17	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) 受权限保护，但应检查权限保护级别。 Permission: android.permission.DUMP [android:exported=true]	警告	检测到 Broadcast Receiver 已导出并受未在本应用定义的权限保护。请在权限定义处核查其保护级别。若为 normal 或 dangerous，恶意应用可申请并与组件交互；若为 signature，仅同证书签名应用可访问。
18	高优先级 Intent（999） -{1} 个命中 [android:priority]	警告	通过设置较高的 Intent 优先级，应用可覆盖其他请求，可能导致安全风险。

代码安全漏洞检测

高危: **3** | 警告: **8** | 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	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
3	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
4	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
5	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
6	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

7	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
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	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
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	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
12	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
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	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
15	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/libesclient.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: ['__strncpy_chk', '__strlen_chk', '__vsprintf_chk', '__strcpy_chk', '__strcat_chk', '__strncat_chk', '__memset_chk', '__FD_SET_chk', '__FD_ISSET_chk', '__vsnprintf_chk', '__memcpy_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
00079	隐藏当前应用程序的图标	规避	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
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

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
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
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
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00175	获取通知管理器并取消通知	通知	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
00036	从 res/raw 目录获取资源文件	反射	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
00092	发送广播	命令	升级会员：解锁高级权限
00039	启动网络服务器	控制 网络	升级会员：解锁高级权限
00128	查询用户账户信息	信息收集 账号	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
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
00163	创建新的 Socket 并连接到它	socket	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
00047	查询本地IP地址	网络 信息收集	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
00134	获取当前WiFi IP地址	WiFi 信息收集	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

00204	获取默认铃声	信息收集	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
00067	查询IMSI号码	信息收集	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
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
00025	监视要执行的一般操作	反射	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.RECEIVE_BOOT_COMPLETED android.permission.WAKE_LOCK android.permission.VIBRATE android.permission.MODIFY_AUDIO_SETTINGS android.permission.SYSTEM_ALERT_WINDOW android.permission.RECORD_AUDIO android.permission.READ_CONTACTS android.permission.WRITE_CONTACTS android.permission.GET_ACCOUNTS android.permission.CALL_PHONE android.permission.READ_CALL_LOG android.permission.WRITE_CALL_LOG android.permission.READ_PHONE_STATE android.permission.PROCESS_OUTGOING_CALLS android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION
其它常用权限	12/46	android.permission.FOREGROUND_SERVICE android.permission.INTERNET android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.BLUETOOTH com.google.android.c2dm.permission.RECEIVE android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS android.permission.READ_EXTERNAL_STORAGE android.permission.READ_MEDIA_AUDIO android.permission.ACCESS_BACKGROUND_LOCATION com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE 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。

恶意域名威胁检测

域名	状态	中国境内	位置信息
ipphone-388ca.firebaseio.com	安全	否	**IP地址:** 34.120.160.131 **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
www.ntt.com	安全	否	**IP地址:** 184.24.29.160 **国家:** 荷兰王国 **地区:** 北荷兰省 **城市:** 阿姆斯特丹 **纬度:** 52.378502 **经度:** 4.899980 **查看:** Google 地图
mobile.ntt.com	安全	否	No Geolocation information available.
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **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

URL 链接安全分析

URL信息	源码文件
• 127.0.0.1	p5/b.java
• http://www.ntt.com	y4/o.java
• https://www.ntt.com/business/services/mobility/ipphone-app/050ip-phone-app/ap_policy.html • https://docs.google.com/viewer?embedded=true&url=	com/ntt/voip/android/com050plus/client/ConfirmPermissionActivity.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	d1/w.java
• https://console.firebase.google.com/	i2/b.java
• 127.0.0.1	m5/y.java
• 127.0.0.1	i5/c.java
• https://mobile.ntt.com/smt/	y3/f.java
• 192.168.1.1	y4/a.java
• https://%s/%s/%s	a2/c.java

• 127.0.0.1	m5/j.java
• 127.0.0.1	t4/a0.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	l1/g.java
• https://ipphone-388ca.firebaseio.com	自研引擎-S
• 2.5.0.1 • 1.4.3.13 • 35.76.73.65	lib/arm64-v8a/libesclient.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://ipphone-388ca.firebaseio.com 的 Firebase 数据库进行通信

Firebase远程配置已启用	警告	Firebase远程配置URL （ https://firebaseremoteconfig.googleapis.com/v1/projects/138822086000/namespaces/firebase:fetch?key=AIzaSyC12M1JvvIVVOTGrgZoP7JbxCkczRaFbQ ） 已启用。请确保这些配置不包含敏感信息。响应内容如下所示：
		{
		"state": "EMPTY_CONFIG",
		"templateVersion": "2"
		}

第三方 SDK 组件分析

SDK名称	开发者	描述信息
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。
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。
Jetpack WorkManager	Google	使用 WorkManager API 可以轻松地调度即使在应用退出或设备重启时仍应运行的可延迟异步任务。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Jetpack 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。

Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。
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。

第三方追踪器检测

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

敏感凭证泄露检测

可能的密钥
"com9921_key_contents_server_http_timeout" : "pref_contents_server_http_timeout"
"com9922_xml_code_key" : "com9922_xml_code_key"
"defval_enable_auth" : "true"
"monitor_key_alarm" : "monitor_key_alarm"
"com9921_key_gcm_request_timeout" : "pref_gcm_request_timeout"
"com9921_key_push_request_retry_interval" : "push_request_retry_interval"
"com9921_key_push_provider_addr" : "pref_push_provider_addr"
"defval_push_call_setting_encode_aes_key" : "J+xPjpqtWE9l8jsb8HXEXHKYM7CT+GtUSRb/gfAfONuOysjfDrIeNyew3Zh5/BwF"
"com.google.firebase.crashlytics.mapping_file_id" : "0e1f298512634b4682e2c3988280cc8f"
"firebase_database_url" : "https://jiggyone-388ca.firebaseio.com"
"com9922_check_timeout_key" : "com9922_check_timeout_key"
"defval_initset_aes_decode_key" : "j9PRtPNgmrt0vOL+K2I21qFgFygheayPbzalIyKgLKE="
"defval_shared_credential" : "true"
"defval_mail_zip_passwd" : "VrgNoe6h5wtdJ3h9C/20Ng=="
"com9922_check_interval_key" : "com9922_check_interval_key"

"com9922_up_code_key" : "com9922_up_code_key"
"google_app_id" : "1:138822086000:android:e283b63a0f048b64"
"defval_firebase_enabled" : "true"
"monitor_key_check_manual_duration" : "monitor_key_check_manual_duration"
"defval_urilink_secret_key" : "MGSbV75R4QScIUMlNDrjuj2aWmPs/L1kibZggzbIHJ8="
"google_crash_reporting_api_key" : "AIzaSyCz2NTJvvIVVOTGrgZoP7J3kxCkczRaFbQ"
"defval_no_blank_auth" : "true"
"monitor_key_incoming_check" : "monitor_key_incoming_check"
"com9902_passwd_dlg" : "Password"
"com9921_key_contents_server_url" : "pref_contents_server_url"
"defval_auth_reg_only" : "true"
"monitor_key_check_interval" : "monitor_key_check_interval"
"monitor_key_check_auto_duration" : "monitor_key_check_auto_duration"
"com9921_key_gcm_request_retry_count" : "pref_gcm_request_retry_count"
"com9923_key_push_call_setting_is_secure" : "pref_puch_setting_is_secure"
"com9921_key_push_email_of_sender" : "pref_push_email_of_sender"
"com9921_key_push_request_retry_count" : "pref_request_retry_count"
"com9923_key_push_call_setting_is_check_cert" : "pref_push_call_setting_is_check_cert"
"defval_max_sessions" : "04qLQkvJFXix0VfPsK/Ig=="
"monitor_key_delete_timer" : "monitor_key_delete_timer"
"monitor_key_check" : "monitor_key_check"
"com9921_key_push_provider_http_timeout" : "pref_push_provider_http_timeout"
"com9902_passwd" : "Password"
"google_api_key" : "AIzaSyCz2NTJvvIVVOTGrgZoP7J3kxCkczRaFbQ"
"com9923_key_puch_call_addr" : "pref_puch_call_addr"
"com9922_check_url_key" : "com9922_check_url_key"
"defval_web_passwd" : "S5xLbyVx3aiOUZe3iAvmtFFA0Ffz5LWrvAj27B7ps1g="
"defval_session_expires" : "iO9XAd9RNXkMDe9Cd1BofQ=="
"defval_crash_zip_password" : "/SHLzkJRSYFkSTI1sK9Rng=="

"com9921_key_push_provider_port" : "pref_push_provider_port"
470fa2b4ae81cd56ecbcda9735803434cec591fa

Google Play 应用市场信息

标题: 050IP電話 - 050番号で携帯□固定への通話がおトク

评分: 2.98 **安装:** 50,000+ **价格:** 0 **Android版本支持:** **分类:** 通讯 **Play Store URL:** com.ntt.voip.android.sdk050voip

开发者信息: NTT DOCOMO BUSINESS, INC., NTT+DOCOMO+BUSINESS,+INC., None, http://www.ntt.com/050voip_sdk/data/image2.html, 050voip_sdk@ntt.com,

发布日期: 2015年8月30日 **隐私政策:** Privacy link

关于此应用:

050 IP电话是我们提供的移动通信服务“移动接入批发商”的主要功能之一。 “移动接入批发”的用户，显示在此应用中，手机的通话记录，请从历史对方，你可以在“050IP电话”的低成本通话费用来源。 此外，我们根本不会将获取的信息发送到外部服务器。 您觉得智能手机上的通话费用是否每30秒一次？ 如果您可以拨打智能手机通话费， 您可以采取更舒适的通话方式。 与移动接入批发相结合也很受欢迎！ ■它可以与移动访问批发商结合使用。 ■这怎么方便使用？ ·使用050号码作为业务用途或子号码的另一个号码 ·利用050电话号码与数据通信SIM合同 ·从海外到日本，可以拨打/收取与日本相同的通话费，方便旅行和商务旅行！ * *有些领域不能被国内外法律引入或使用。由于海外手机分组通信费用可能很高，我们建议使用海外免费统一费率服务和免费Wi-Fi现货。 *有关如何使用此应用程序和合同的详细信息，请联系每个提供商。 【050 IP电话的主要功能】 ·IP电话（呼叫/接收），电话号码从050开始 ·手机通话显示历史显示功能 ·从手机拨号盘（智能手机）拨打电话时 通过切换到050 IP电话轻松切换功能 ·手机通话捕捉功能 ·键盘更换功能 ·铃声变化功能 ·电话簿组功能 ·免费通话目的地050号码识别功能 ·静音功能，扬声器功能，保持功能 ·网络监控功能 ■接收电话和电子邮件时产生的分组通信费用由客户承担。我们建议使用数据包统一费率服务。 【关于合同】 有关如何使用此应用程序和合同的详细信息，请联系每个提供商。 引用的信息不会传输到外部服务器。 050 IP许可协议使用条款（Android） 第1条（050 IP电话应用许可协议的条款和条件的目的） 1 050 IP许可协议申请的使用条款（以下简称“许可协议”）是“050 IP电话申请（”）以下称为“本申请”。 2安装和使用本应用程序的人员（以下简称“用户”）应诚意遵守本许可证。 第2条（本许可证的适用范围） 1本许可证适用于您与我们之间与本申请相关的所有关系。 不管前面的设备中，根据使用的用户的应用程序（以下简称为“电信服务供应商”）。电信服务供应商中的间，电信服务使用根据使用本申请的如果订立合约时和在其上输入的合同到，任何关系相对于本申请中，是日期之后由于术语诸如电信服务提供商定义。 第3条（本申请的使用许可） 1我们授予您使用本应用程序的权利。但是，不授予用户有关公司商标，商号或服务标记的任何权利。 2用户可以在我们确认本应用程序操作的终端（以下简称“终端”）上安装和使用终端。这里，用于使该应用程序在终端上运行。 请在主页上查看最新的应用程序操作检查条件（将列出050 IP URL应用程序）。 第4条（本申请的禁止事项） 1用户不得为使用本应用程序所需的范围内复制本应用程序的全部或部分内容，除非是备份目的。 2用户不得修改此应用程序的全部或部分内容。 3用户不得对本应用程序中包含的软件程序进行反向工程，反汇编，反编译等。 第5条（本申请的变更） 1公司，在未取得用户同意，有权可以改变这个应用程序的内容（包括本应用程序的版本升级。）它应能执行。 2本许可协议和本申请的变更应在本申请提供网站上发布时生效。 第6条（取消和中断本申请） 1我们可以暂停或暂停使用本申请（以防止临时使用，以下同样适用）。 （1）升级此应用程序时 （2）当该应用程序不能正常运行时，很难连续提供此应用程序 第7条（终止我们提供的此申请） 1公司应能够终止本申请的提供。在这种情况下，我们不对用户或任何其他人承担任何责任。 第8条（知识产权的归属） 1与本申请及其相关文件相关的版权和其他知识产权属于我们。 2此应用程序使用libSRTP。有关许可条款，请访问（http://srtp.sourceforge.net/license.html）。 3此应用程序使用Apache commons日志记录，Apache Commons编解码器。 有关许可条款（http://www.apache.org/licenses/LICENSE-2.0.html），请访问。 4此应用程序使用Zip4j。有关许可条款，请访问（http://www.lingala.net/zip4j/）。 第9条（我们公司的免责声明） 1我们不对用户承担任何责任。 （1）本申请不侵犯他人的权利 （2）什么可以用于任何终端 （3）其有用户期望的质量，操作不被中断，操作中没有错误 （4）不要对安装此应用程序的终端中的其他应用程序和用户数据产生负面影响 前款，本公司，当使用该应用程序的用户，或任何第三方的情况除外，本公司故意或重大过失的，不承担任何责任的另一种简称。此外，公司从该公司造成的损失，就行为依照本协议的规定，都不应该承担任何责任。 第10条（用户自己的责任） 1个用户，当使用的应用程序，如果必须改变已经发生端子的设置，或者如果设定等由应用程序自动地改变，所产生的费用改变其配置，例如，我们将承担自己的责任和负担，我们不承担任何责任。 第11条（用户应遵守的事项） 1个用户，该技术在此应用程序和该应用程序使用（以下简称“应用等”。）在使用，外汇及外贸管理法和其他日本出口相关的法律法规，以及，美国出口管理条例出口有受到基于潜在的监管，以及对认识到有可能是与主题相关的其他国家出口法规，并应符合这些法律所规定的，还有，这个应用程序等，没有相应的政府许可，禁运国家或贸易制裁的国家企业，居民，国家，或交易违禁的人，反对贸易禁令公司，转让，那些不出口或再出口我会的，2级的用户，该应用程序或类似大规模毁灭性武器，包括在外汇和外国贸易法等日本出口相关的法律法规，这种常规武器，制造业的发展定义是核武器，并不得可供使用。 ※本应用程序下载，原产于这个应用程序，来料，分组通信的互联网连接，如呼叫自费，我们建议，因为它成为你的负担，用户使用数据包包月服务。另外，应用程序可以周期性地执行自动通信，并且还将产生分组通信费用。

免责声明及风险提示:

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。