MoGua

Mini语音 2.4.0.APK 分析报告

APP名称:	Mini语音

包名:	com.miniapp.talk
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年8月3日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app-release.apk
文件大小: 36.2MB
MD5值: 1389cc4e2ef4ad8f7bdee8add04c4f16
SHA1值: 377980e66873c24452593024581f6800cab490b2
SHA256值: 365a7e87e6921744294af249808a7776b030d8f12f3d506bb154834257a0c016

APP 信息

App名称: Mini语音
包名: com.miniapp.talk
主活动Activity: com.miniapp.talk.activity.LunchActivity
安卓版本名称: 2.4.0
安卓版本: 104

域名线索

域名	服务器信息
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

URL线索

URL信息	Url所在文件
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎

https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=710000, ST=shaanxi, L=xian, O=shuzituteng, OU=zhiyuantian, CN=Mythe Tian
签名算法: rsassa_pkcs1v15
有效期自: 2016-03-15 05:49:32+00:00
有效期至: 2041-03-09 05:49:32+00:00
发行人: C=710000, ST=shaanxi, L=xian, O=shuzituteng, OU=zhiyuantian, CN=Mythe Tian
序列号: 0x54676353
哈希算法: sha256
md5值: d785777d12cb1c45600b7fb886e81f47
sha1值: ed5787505aa74217a5d132eae52a142dd62272dc
sha256值: b345baeb38975d6bd26d2d1f43203b75ee7c5be0aa4138f8b136473ef56630e1
sha512值: 84e174a49e2030d71eb02f9446fa2368983a39d0ff528f6167316d1b3e7330fa90e5156e26980a20e676926395b66a9a7d1c7eacef9453e110a63dadd7ee4cc6
公钥算法: rsa
密钥长度: 2048
指纹: fd2c22a79fa665331428c66d2106cddeb02e721cd563896c52bc8860143fb1ad

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"
"rc_authorities_fileprovider" : ".FileProvider"
"rc_conversation_list_my_private_conversation" : "我的私人会话"
"rc_emoji_hear_no_monkey" : "不听"
"rc_emoji_see_no_monkey" : "不看"
"rc_conversation_list_my_private_conversation" : "My private conversation"
"rc_emoji_hear_no_monkey" : "Hear-No-Monkey"
"rc_emoji_see_no_monkey" : "See-No-Monkey"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	

		URL**链接**
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.READ_EXTERNAL_STORAGE	危险	读取外部存储器内容	允许应用程序从外部存储读取
android.permission.ACCESS_NETWORK_STATE	正常	查看网络状态	允许应用程序查看所有网络的状态
android.permission.ACCESS_WIFI_STATE	正常	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	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备

android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
com.miniapp.talk.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量

android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent100424468://,
