MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

TreeTalk 0.9.6.APK

APP名称:	TreeTalk
包名:	cn.dostudio.app.treetalk
域名线索:	6条
URL线索:	3条
邮箱线索:	1条
分析日期:	2022年1月28日 23:19

文件信息

文件名: treetalk.apk
文件大小: 11.9MB
MD5值: 9d8eaebd5c1adf424bd8dcee987bc475
SHA1值: 0636b5ee7c60b00de618d983f3237a2f61bd8f58
SHA256值: f4d43db6844e922014b29f8ee5bbc7ac6005ac2d083d5d4299242f97549f0a46

APP 信息

App名称: TreeTalk
包名: cn.dostudio.app.treetalk
主活动**Activity:** cn.dostudio.app.treetalk.ui.activity.SplashActivity
安卓版本名称: 0.9.6
安卓版本: 10

域名线索

域名	是否危险域名	服务器信息
errlogos.umeng.com	good	**IP:** 47.246.110.18 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
appgallery.cloud.huawei.com	good	**IP:** 49.4.35.33 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
errlog.umeng.com	good	**IP:** 111.225.159.19 **所属国家:** China **地区:** Hebei **城市:** Zhangjiakou **纬度:** 40.810001 **经度:** 114.879440 **查看地图:** Google Map
store.hispace.hicloud.com	good	**IP:** 49.4.19.250 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map
play.google.com	good	**IP:** 172.217.163.46 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map

域名	是否危险域名	服务器信息
www.mob.com	good	**IP:** 116.62.130.46 **所属国家:** China **地区:** Beijing **城市:** Beijing **纬度:** 39.907501 **经度:** 116.397232 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
http://www.mob.com/policy/en	Android String Resource
http://www.mob.com/about/policy	Android String Resource
https://www.mob.com	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
http://www.mob.com/policy/zh	Android String Resource
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so

URL信息	Url所在文件
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libconscrypt_jni.so

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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。

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
cn.dostudio.app.treetalk.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
cn.dostudio.app.treetalk.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
cn.dostudio.app.treetalk.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=zhejiang, L=hangzhou, CN=Treetalk
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-09 08:24:56+00:00
Valid To: 2046-08-03 08:24:56+00:00
Issuer: C=CN, ST=zhejiang, L=hangzhou, CN=Treetalk
Serial Number: 0x7e9a3d8c

Hash Algorithm: sha256
md5: 92c21bb2f687104a42d48338b4f8f112
sha1: 991f760bdb595156d1a56291535c1758a1a182c1
sha256: 7379dc4b1b3acf9ac4b4daadfa3794e2907007f8b14506b2bc49330f262bdf42
sha512: f8eb90187764632021a34a76cc3e25f7e8006fa9e034e1613baebabe031ac745d16affe6c4a6e3db5899b218063bae56237f3308eeb902074c962614aa834490
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 39108999812153df8e1edb8a25c0230cbfe623ff4f514319a960670c02b6be38

硬编码敏感信息

可能的敏感信息
"about_author" : "Android 轮子哥"
"btg_login_password" : "Password"
"btg_login_username" : "Account"
"login_private_protocol" : "隐私政策"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"mobdemo_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/about/policy。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"

可能的敏感信息
"mobdemo_authorize_dialog_title" : "服务授权"
"real_auth" : "实名认证"
"search_tab_user" : "用户"
"search_user_name" : "搜索用户名"
"setting_password" : "修改密码"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"
"mobcommon_authorize_dialog_title" : "服务授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
cn.dostudio.app.treetalk.biz.tree.LeafDetailActivity	Schemes: appTreeTalk://, Hosts: treetalk.cn, Paths: /leafDetail,
cn.dostudio.app.treetalk.biz.tree.BranchActivity	Schemes: appTreeTalk://, Hosts: treetalk.cn, Paths: /treeBranch,
cn.dostudio.app.treetalk.biz.setting.BlackListActivity	Schemes: appTreeTalk://, Hosts: treetalk.cn, Paths: /blackList,
cn.dostudio.app.treetalk.ui.activity.SplashActivity	Schemes: xi4pvqwck://,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencentxx://,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Jiagu

文件列表	分析结果
classes.dex	壳列表 | 详细情况 编译器 | dexlib 2.x
