MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

新宏 1.0.5.APK

APP名称:	新宏
包名:	com.xinhong.app
域名线索:	3条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年1月25日 22:56

文件信息

文件名: xinhong565304.apk
文件大小: 4.87MB
MD5值: a14fffba24533f7bea0ef6ac2faf9a57
SHA1值: e95dbb575dedc849d6e2b93d84d7d50e8ccf7d28
SHA256值: db59a8709c44a83af0e37920e96682f2d56a0f0e18ca3e490c409b73eb0cdf0c

APP 信息

App名称: 新宏
包名: com.xinhong.app
主活动**Activity:** com.lt.app.MainActivity
安卓版本名称: 1.0.5
安卓版本: 105

域名线索

域名	是否危险域名	服务器信息
store.hispace.hicloud.com	good	**IP:** 124.70.117.217 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map

域名	是否危险域名	服务器信息
play.google.com	good	**IP:** 172.217.160.110 **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
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **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
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。

向手机申请的权限	是否危险	类型	详细情况
com.xinhong.app.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
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
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.xinhong.app.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.xinhong.app.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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
com.xinhong.app.permission.techain.RECEIVE	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.xinhong.app.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.xinhong.app.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.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference
com.xinhong.app.permission.YM_APP	未知	Unknown permission	Unknown permission from android reference
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_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=ZF, ST=ZF, L=ZF, O=ZF, OU=ZFFP, CN=ZF
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-04 06:42:00+00:00
Valid To: 2121-11-10 06:42:00+00:00
Issuer: C=ZF, ST=ZF, L=ZF, O=ZF, OU=ZFFP, CN=ZF
Serial Number: 0x3942d013
Hash Algorithm: sha256
md5: e279507d648ececb6aa1d31b6fa011ff
sha1: 44721f045fd36f752d620965abce73b97a1e0911
sha256: b6392fa60bff59dd61f747c728af2d1a491936887d185a8bd39a851b2c687e95
sha512: 15aa647545dd422f89f517a64aaca7d46b1a6ee82ace46248b486dfcecb9586a0cc6518e74379498a10c3b3c11a1c4bfbf2006e2d7bfb205dd5ea788b97b8320
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 7b86d5b790ce8a1b06f2799654d9560b7a43d447c0e43aa46f12bc9fc46ed257

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"p_ht_appkey" : "700025095"
"p_ht_mz_appkey" : ""
"p_ht_op_appkey" : ""
"p_ht_op_appsecret" : ""
"p_ht_vv_appkey" : ""
"p_ht_xm_appkey" : ""
"p_rcpush_mzAppKey" : ""
"p_rcpush_opAppKey" : ""
"p_rcpush_opAppSecret" : ""
"p_rcpush_vvAppKey" : ""
"p_rcpush_xmAppKey" : ""
"p_u_appkey" : "61ab0db9e014255fcb9bf602"
"p_weibo_appkey" : ""

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.lt.app.JumpActivity	Schemes: ltapp281203://,
com.baidu.techain.push.VivoPushActivity	Schemes: vpushscheme://, Hosts: com.xinhong.app, Paths: /detail,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机: Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check 编译器: r8 模糊器: unreadable field names unreadable method names

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/arm64-v8a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
<tr><td>lib/armeabi-v7a/libtechain.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>模糊器</td><td>Obfuscator-LLVM version 3.4</td></tr>
</table>
</td></tr>
</table>
