MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

悬赏客 1.0.0.APK

APP名称:	悬赏客
包名:	com.app.xuanshangke
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2022年1月20日 22:18

文件信息

文件名: xuanshangke.apk
文件大小: 8.77MB
MD5值: bbef8679005d6b447650a71dac8a6a78
SHA1值: 17811d659d29bf38bb3e3ea6abe3b5c88f76ecaf
SHA256值: c15ecb44b513a5d68a68d3eb4af937a8c3d74f27aab1e6be39a3e5002cf90cdb

APP 信息

App名称: 悬赏客
包名: com.app.xuanshangke
主活动**Activity:** com.app.xuanshangke.common.activity.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 1

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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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
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.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.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

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.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.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.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
com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼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.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
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。
com.huawei.android.launcher.permission.READ_SETTINGS	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
com.huawei.android.launcher.permission.WRITE_SETTINGS	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
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	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
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
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.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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: C=086, ST=zhejiang, L=hangzhou, O=juejia, OU=juejia, CN=xuanshangke
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-29 03:41:41+00:00
Valid To: 2069-11-16 03:41:41+00:00
Issuer: C=086, ST=zhejiang, L=hangzhou, O=juejia, OU=juejia, CN=xuanshangke
Serial Number: 0x7462fcf5
Hash Algorithm: sha256
md5: 1634147d005d47e8b670df3ff3bc4ab7
sha1: 26f45650d5bb2265faa6579b58bed1d7aefaa7a0
sha256: 8d2662b151c46533382bca282f3c06ea86e1c47147227b14fc7bda0932d91691
sha512: 50770ee5d29d65a57af55d98b6b83fc81f271c29696b100251befd71fd3a95e6f33f206819ec6f56fb9c93bf2a9212e2183df4156f9746faed6c103003227c0a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 69ee4891ccff1253db30dac2dd56be8ffa2c74b7a6f7443587e082361c3fa110

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.app.xuanshangke.common.activity.SplashActivity	Schemes: xuanshangke://, Hosts: juejia.com,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>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
network interface name check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
lib/arm64-v8a/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/armeabi-v7a/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/armeabi/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/x86/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
lib/x86_64/libnms.so	壳列表 | 详细情况 模糊器 | ByteGuard 0.9.3
