MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

小鹿助手 2.0.7.APK

APP名称:	小鹿助手
包名:	com.hna.mobile.android.deerjet.mydeer
域名线索:	4条
URL线索:	7条
邮箱线索:	0条
分析日期:	2022年2月3日 12:44

文件信息

文件名: xlzs.apk
文件大小: 5.79MB
MD5值: f466e88229ec8ce0ec7d333115449c42
SHA1值: ecafe7208ade23013e83f8771b6253476fcaac12
SHA256值: b567a61daf5f2755e25e6030db98cbe8075177b3490f385adf75f6e98020f77e

APP 信息

App名称: 小鹿助手
包名: com.hna.mobile.android.deerjet.mydeer
主活动**Activity:** MainActivity
安卓版本名称: 2.0.7
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
nav.cn.ronghub.com	good	**IP:** 140.143.50.86 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

域名	是否危险域名	服务器信息
stats.cn.ronghub.com	good	**IP:** 106.75.5.96 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
mbp.deerjet.com	good	**IP:** 106.120.129.69 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
www.hnastore.com下载最新版小鹿助手	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://mbp.deerjet.com:9603/mobi/version?type=android	com/hna/mobile/android/deerjet/mydeer/plugin/AppVersionControl.java
www.hnastore.com下载最新版小鹿助手	com/hna/mobile/android/deerjet/mydeer/plugin/AppVersionControl.java
http://nav.cn.ronghub.com/navipush.json	io/rong/push/PushConst.java
https://stats.cn.ronghub.com/active.json	io/rong/imlib/RongIMClient.java

URL信息	Url所在文件
http://nav.cn.ronghub.com/navi.xml	lib/armeabi-v7a/libRongIMLib.so
http://nav.cn.ronghub.com/navi.xml	lib/x86/libRongIMLib.so
http://nav.cn.ronghub.com/navi.xml	lib/arm64-v8a/libRongIMLib.so
http://nav.cn.ronghub.com/navi.xml	lib/armeabi/libRongIMLib.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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
com.hna.mobile.android.deerjet.mydeer.permission.JPUSH_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
android.permission.RECEIVE_USER_PRESENT	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
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=beijing, L=beijing, O=MyDeer, OU=MyDeer, CN=MyDeer
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-07-07 02:11:57+00:00
Valid To: 2040-06-30 02:11:57+00:00
Issuer: C=cn, ST=beijing, L=beijing, O=MyDeer, OU=MyDeer, CN=MyDeer
Serial Number: 0x4d94659d

Hash Algorithm: sha256
md5: 7e8ddcfa4b144a6c118a911a42bc3783
sha1: 6ed4ce4038a1de5e68083c7bbf64acfe77a4cd59
sha256: 672ddc0c07e4b9f0e553ec542e4484f5af7d6cc49f49e1af7f51ddd3028554e5
sha512: 6e4c15c3f013a4cef3817043c30bcfcc27d00842be214d985295c083113d1a6f482d5c584bedfda57a773f6b7115c2eefa17c2feb0a463d3000c0f9f16d74c25

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<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.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check network operator name check device ID check subscriber ID check</td></tr><tr><td>反调试</td><td>Debug.isDebuggerConnected() check</td></tr><tr><td>编译器</td><td>dx (possible dexmerge)</td></tr><tr><td>Manipulator Found</td><td>dexmerge</td></tr></table>
