MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

大牛设计 2.0.APK

APP名称:	大牛设计
包名:	com.yunye.daniusheji
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2022年2月2日 19:43

文件信息

文件名: dnsj.apk
文件大小: 7.24MB
MD5值: d704a70b5dfca3b5c20b1764959f1cb8
SHA1值: fc1793ad1559cca49c135a09c66d0a69c8381b28
SHA256值: 045dbc1f6888b9a9a26c55b85ade2363dc4503274b351ddeca412fee78185ca0

APP 信息

App名称: 大牛设计
包名: com.yunye.daniusheji
主活动**Activity:** com.yunye.ui.main.MainActivity
安卓版本名称: 2.0
安卓版本: 20

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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

向手机申请的权限	是否危险	类型	详细情况
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.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.yunye.daniusheji.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.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.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.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: CN=gao
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-11-24 04:04:14+00:00
Valid To: 2042-11-18 04:04:14+00:00
Issuer: CN=gao
Serial Number: 0x6e24cb3
Hash Algorithm: sha256
md5: a3cdcc102583e1c4057112f5407c57f2
sha1: 8de1019cd753201055ea4d48069ff412fccf691b
sha256: 277a14211ad968f2b9a4a52d26597fccde4a864d213d231690465f12d6d3109a
sha512: e378f9e4b1a3c3b35e554499473b85288da26675f0102b5142c24055d09dd1248bf00db0ad85db2d282eb8e423132177eb10f631132b19bdc957fc5aec72a0f4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 56efa4a6476359326731ebd262d3897e90111ecf2544f2cf89d4c0603939469d

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>APK包</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>打包</td><td>Jiagu</td></tr>
</table>
</td></tr>
</table>

<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>编译器</td><td>dexlib 2.x</td></tr>
<tr><td>模糊器</td><td>unreadable field names
unreadable method names</td></tr>
</table>
</td></tr>
</table>
