MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

爱云赞福利 3.14.01.APK

APP名称:	爱云赞福利
包名:	com.shoujizhuan.jiayou
域名线索:	1条
URL线索:	1条
邮箱线索:	0条
分析日期:	2022年2月2日 11:35

文件信息

文件名: aiyunzanapp.apk
文件大小: 13.09MB
MD5值: 8c34efe502a63e35a9837f8ac37b8bbb
SHA1值: bda6cab8458999ef07d3c33d1d66b2168dfd43b4
SHA256值: 085a7039bd759d018eff447cb47c0b7803cdb3e0aa5ba98267e491f811173b83

APP 信息

App名称: 爱云赞福利
包名: com.shoujizhuan.jiayou
主活动**Activity:** com.lushi.duoduo.start.ui.SplashActivity
安卓版本名称: 3.14.01
安卓版本: 31401

域名线索

域名	是否危险域名	服务器信息
a.tn990.com	good	**IP:** 125.39.76.190 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://a.tn990.com/app.apk	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.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.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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
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.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.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_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.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.SYSTEM_OVERLAY_WINDOW	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.KILL_BACKGROUND_PROCESSES	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

向手机申请的权限	是否危险	类型	详细情况
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.INSTANT_APP_FOREGROUND_SERVICE	系统需要		允许免安装应用创建前台服务
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.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
com.shoujizhuan.jiayou.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
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.asus.msa.SupplementaryDID.ACCESS	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.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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=HuBei, L=WH, O=Ls, OU=VideoB, CN=Xuxiong
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-29 02:01:38+00:00
Valid To: 2075-04-02 02:01:38+00:00
Issuer: C=CN, ST=HuBei, L=WH, O=Ls, OU=VideoB, CN=Xuxiong
Serial Number: 0x31194e59
Hash Algorithm: sha256
md5: 032d876edc11eb0414b8ba65544fb3d3
sha1: 2ff23cae01c08d9527d7cb1df4663ba837b0f955
sha256: 20bdc8b851ef992684c7704bfcd8387b84f1b237712a22cfdabd766d9f0852a6
sha512: db4a507f38fcb2092b0288c093e07724295e971bedf5aaab21c575ae399af86a63fd5258c3161c388c54a73be6b9d34eb6c9094422c51c4371ced340a1344f35

应用内通信

活动(ACTIVITY)	通信(INTENT)

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1109118142://,

加壳分析

文件列表	分析结果
APK包	壳列表 / 详细情况 打包 / Tencent's Legu
assets/gdt_plugin/gdtadv2.jar!assets/yaq3_0.sec	壳列表 / 详细情况 反虚拟机 / Build.MODEL check 编译器 / dexlib 2.x

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!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.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
possible Build.SERIAL check
subscriber ID check</td></tr>
<tr><td>编译器</td><td>dexlib 2.x</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/armeabi/libturingau.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 unknown</td></tr>
</table>
</td></tr>
<tr><td>assets/gdt_plugin/gdtadv2.jar!lib/arm64-v8a/libturingau.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 unknown</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>lib/armeabi-v7a/libnms.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>模糊器</td><td>ByteGuard 0.9.3</td></tr></table></td></tr>
<tr><td>lib/armeabi/libnms.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>模糊器</td><td>ByteGuard 0.9.3</td></tr></table></td></tr>
<tr><td>lib/x86/libnms.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>模糊器</td><td>ByteGuard 0.9.3</td></tr></table></td></tr>
<tr><td>assets/libshellx-super.2019.so</td><td><table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>emulator file check</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>unknown (please file detection issue!)</td></tr></table></td></tr>
</table>

文件列表	分析结果
classes.dex	壳列表 / 详细情况 防止反汇编: non-zero link size non-zero link offset 打包: Mobile Tencent Protect 编译器: dexlib 2.x

---