MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

积加ERP 1.0.0.APK

APP名称:	积加ERP
包名:	com.yunjian.erp_android
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 20:27

文件信息

文件名: jjerp498767.apk
文件大小: 6.86MB
MD5值: 61cd4c1b21aba2993b006f064b6e7983
SHA1值: a1963b8119b7d4afd21e7c13795c99d9d5998c04
SHA256值: 2c19502bd2d03d876d9317cfae5f884b31ed6ddfd5ed707061023e26ebb91140

APP 信息

App名称: 积加ERP
包名: com.yunjian.erp_android
主活动**Activity:** com.yunjian.erp_android.allui.activity.splash.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 72

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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
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_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_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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.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.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.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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.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.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。

向手机申请的权限	是否危险	类型	详细情况
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.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。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=ji
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-07-13 11:34:17+00:00
Valid To: 2046-07-07 11:34:17+00:00
Issuer: CN=ji
Serial Number: 0x2a0d79e7
Hash Algorithm: sha256
md5: 82e2c83e16adf4793ca25ea9c9a1eb3d
sha1: 2999b890d0f37b403cbab325710b2b42f0820ec1
sha256: 494601c6614ee383fc2a2509ac20df7de7cc3f8721cd6b7cfda236087320307f
sha512: 97055d615fd81aaf0ec5e33a3d4d9e854cb648fc7990ec68e815e5131409ce9420ac3b9452b4c639be6648413af5ba80b10db8087d2e186459d98b49e2c98c91
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c437788123e610aad548ff29631c4ae0fc35a8cb867b1db27dadbd6ed314f0ae

Exodus威胁情报

名称	分类	URL链接
Baidu Mobile Stat	Analytics	https://reports.exodus-privacy.eu.org/trackers/101

硬编码敏感信息

可能的敏感信息
"login_api" : "请输入登录链接前缀"
"protocol_user" : "用户协议"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.yunjian.erp_android.allui.activity.splash.SplashActivity	Schemes: mtj98783b1406://,

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></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>
<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.BOARD check
device ID check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
