MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

财运达 V1.0.0.APK

APP名称:	财运达
包名:	com.sxzjhc.carrier
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 19:28

文件信息

文件名: caiyunda.apk
文件大小: 5.49MB
MD5值: d1debf5a5b4f9b1944f241edd0c86a0d
SHA1值: f006fedf67775b7079a5536a68717416b5932ce5
SHA256值: d7307e4994922c42441aa7d35e568465cd1bbc6bff211c45fff31b0bbcc31a1d

APP 信息

App名称: 财运达
包名: com.sxzjhc.carrier
主活动**Activity:** com.wurunhuoyun.carrier.ui.activity.SplashActivity
安卓版本名称: V1.0.0
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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_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.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_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.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
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=zhongjinhuichuang
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-09 06:01:49+00:00
Valid To: 2119-06-16 06:01:49+00:00
Issuer: CN=zhongjinhuichuang
Serial Number: 0x3d8afd0
Hash Algorithm: sha256
md5: 1f1ac51c4606d0a102a430fba3941919
sha1: 5b901957c43308813cf6506d1aa22f09e2f13e77
sha256: 864ecdb34c67e123754e52ac3cda5cfd02aab6daf2e06f0131b8d9b7e872c83b
sha512: f05fffcc072e046d729fd7847c2e8e20b657d79c24db0d3801970216aea2afc51c73371bb9179bea6bf9c9f5d6a0cdae99965a22013bdb8f37d5a249f91145fd
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a11ae33525a9d98c539fcf185645df46f0d6fe6a7f45f33a19afd93bfc6fbc01

硬编码敏感信息

可能的敏感信息
"find_password" : "找回密码"
"forget_password" : "忘记密码"
"forget_pwd" : "忘记密码"
"identity_authentication" : "身份认证"
"please_input_password" : "请输入密码"
"please_input_pwd" : "请输入密码"
"please_set_login_pwd" : "请设置登录密码"
"pwd_char_range" : "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKMLNOPQRSTUVWXYZ0123456789"
"reset_authentication" : "重新认证"
"reset_pwd_success" : "重置密码成功"
"set_pwd" : "设置密码"
"setting_pwd" : "正在设置密码"
"user_name" : "昵称"

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>
<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>
