MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

SoonWon 1.2.APK

APP名称:	SoonWon
包名:	com.soonec.won
域名线索:	3条
URL线索:	10条
邮箱线索:	0条
分析日期:	2022年2月2日 22:38

文件信息

文件名: soonwon515346.apk
文件大小: 3.08MB
MD5值: 46b37ef933f655a1c8bfc70f06b296a0
SHA1值: df9379df1e9eb57aebf244656607f3cf56f46752
SHA256值: cef3954fb4325d3514aec136ba24ba342e51c8955d098501cf52047b3a26c14c

APP 信息

App名称: SoonWon
包名: com.soonec.won
主活动**Activity:** com.soonec.won.WelcomeActivity
安卓版本名称: 1.2
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
won.soonec.com	good	**IP:** 120.77.42.16 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 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
open.weixin.qq.com	good	**IP:** 175.24.209.30 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

URL线索

URL信息	Url所在文件
https://won.soonec.com/update.htm	com/soonec/won/SoonWonActivity.java
https://won.soonec.com/update/download.htm	com/soonec/won/SoonWonActivity.java
https://won.soonec.com	com/soonec/won/Config.java
https://won.soonec.com	com/soonec/won/JSInterface.java
https://won.soonec.com/update	com/soonec/won/UpdateActivity.java

URL信息	Url所在文件
https://won.soonec.com/update/download	com/soonec/won/UpdateActivity.java
https://won.soonec.com/update.htm	com/soonec/won/WelcomeActivity.java
https://won.soonec.com/update/hot.htm	com/soonec/won/WelcomeActivity.java
https://won.soonec.com	com/soonec/won/utils/NetUtil.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.CALL_PRIVILEGED	系统需要	直接拨打任何电话号码	允许应用程序拨打任何电话号码,包括紧急电话号码,而无需您的干预。恶意应用程序可能会向紧急服务发出不必要和非法的呼叫
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=GD, L=GZ, O=soonec, OU=com, CN=won
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-02 07:39:04+00:00
Valid To: 2046-09-26 07:39:04+00:00
Issuer: C=CN, ST=GD, L=GZ, O=soonec, OU=com, CN=won
Serial Number: 0x7391bf9f
Hash Algorithm: sha256
md5: 04a43617793e9bf045b54aee765d7313
sha1: 95edcc76e5f927166953ae3982e1e41f1515f4c1
sha256: 00fdf3bb48ab896a8c15d4580d29f4e8ee87f4789ae3891b9510fa9c2c5adf29
sha512: 1c8cd5279c7351016f4b8c9225276040defed9c4cd21239fb6cb7e26ff3b0e35e1ac82faf8f2cfeb18c27ea78e5fb8b9229d4afd8061b0789cd27a368a573307
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 387b6841bec241d507cec7cdc6a551b762d329f4c59a11df66569832dcbae9ef

加壳分析

文件列表	分析结果
classes.dex	壳列表 | 详细情况 编译器 | r8
