MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

安心扫描大师 1.0.1.APK

APP名称:	安心扫描大师
包名:	com.joiya.scanner
域名线索:	25条
URL线索:	20条

邮箱线索:	0条
分析日期:	2022年2月2日 17:02

文件信息

文件名: axsmds426440.apk
文件大小: 4.97MB
MD5值: 3c169619ec49e60c2ff01a7b3b061f12
SHA1值: 06da73b8eb630f99f4c1277d8eabe4d6b6aec44c
SHA256值: 73aba08cad1fe7405d39a56ed6c3325e88e1994bddf542e08851a4d6f50f1c52

APP 信息

App名称: 安心扫描大师
包名: com.joiya.scanner
主活动Activity: com.joiya.scanner.ui.SplashActivity
安卓版本名称: 1.0.1
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
ichannel.snssdk.com	good	**IP:** 125.39.216.237 **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

域名	是否危险域名	服务器信息
toblog.ctobsnssdk.com	good	**IP:** 42.81.156.229 **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
shenghuo.xiaomi.com	good	没有服务器地理信息.
schemas.android.com	good	没有服务器地理信息.
databyterangers.com.cn	good	没有服务器地理信息.
astat.bugly.cros.wr.pvp.net	good	**IP:** 170.106.135.32 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418 **查看地图:** Google Map
rtlog.snssdk.com	good	**IP:** 119.96.137.228 **所属国家:** China **地区:** Hubei **城市:** Wuhan **纬度:** 30.583330 **经度:** 114.266670 **查看地图:** Google Map
log.reyun.com	good	**IP:** 71.131.218.10 **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
clean.kunyumobile.com	good	**IP:** 118.178.85.41 **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
rtapplog.snssdk.com	good	**IP:** 125.39.135.216 **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
img.zcool.cn	good	**IP:** 125.39.76.194 **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
xml.apache.org	good	**IP:** 151.101.2.132 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
astat.bugly.qcloud.com	good	**IP:** 150.109.29.135 **所属国家:** Korea (Republic of) **地区:** Seoul-teukbyeolsi **城市:** Seoul **纬度:** 37.568260 **经度:** 126.977829 **查看地图:** Google Map
image.kunyumobile.com	good	**IP:** 125.39.43.241 **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
ns.adobe.com	good	没有服务器地理信息.
appservice.2363nice.com	good	**IP:** 39.102.31.84 **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
applog.snssdk.com	good	**IP:** 119.96.137.224 **所属国家:** China **地区:** Hubei **城市:** Wuhan **纬度:** 30.583330 **经度:** 114.266670 **查看地图:** Google Map
toblog-alink.ctobsnssdk.com	good	**IP:** 140.249.89.226 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **查看地图:** Google Map
log.snssdk.com	good	**IP:** 27.185.6.215 **所属国家:** China **地区:** Hebei **城市:** Shijiazhuang **纬度:** 38.041389 **经度:** 114.478607 **查看地图:** Google Map
tobapplog.ctobsnssdk.com	good	**IP:** 42.81.156.229 **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
android.bugly.qq.com	good	**IP:** 109.244.244.35 **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
long.open.weixin.qq.com	good	**IP:** 109.244.217.35 **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

域名	是否危险域名	服务器信息
open.weixin.qq.com	good	**IP:** 175.24.219.72 **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
success.ctobsnssdk.com	good	**IP:** 140.249.90.209 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **查看地图:** Google Map
jisulog.sortda.com	good	**IP:** 140.179.91.110 **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
http://xml.apache.org/xslt}indent-amount	com/blankj/utilcode/util/g.java
http://clean.kunyumobile.com/tracer/auditor	com/user/common/UserSourceManager.java
http://clean.kunyumobile.com/tracer/reyun/query	com/user/common/UserSourceManager.java
http://clean.kunyumobile.com/tracer/query	com/user/common/UserSourceManager.java
https://log.reyun.com/receive/pkginfo	com/reyun/tracking/utils/HttpNetworkUtil.java
https://jisulog.sortda.com/	com/reyun/tracking/common/ReYunConst.java
https://shenghuo.xiaomi.com/v5/index.html?statusBarColor=ffffff#page=hotSale&from=zhanwai&pageId=776&pageName=%E7%88%86%E5%93%819%E5%9D%979&outerIndex=1&cheapIndex=0&fullScreen=1&media=WBMT	com/re/co/b/RemoteConfig.java
https://img.zcool.cn/community/01b72057a7e0790000018c1bf4fce0.png	com/joiya/module/scanner/ui/home/HomeFragment.java
https://img.zcool.cn/community/016a2256fb63006ac7257948f83349.jpg	com/joiya/module/scanner/ui/home/HomeFragment.java

URL信息	Url所在文件
https://img.zcool.cn/community/01233056fb62fe32f875a9447400e1.jpg	com/joiya/module/scanner/ui/home/HomeFragment.java
https://img.zcool.cn/community/01700557a7f42f0000018c1bd6eb23.jpg	com/joiya/module/scanner/ui/home/HomeFragment.java
https://img.zcool.cn/community/01b72057a7e0790000018c1bf4fce0.png	com/joiya/scanner/ui/GuideActivity.java
https://img.zcool.cn/community/016a2256fb63006ac7257948f83349.jpg	com/joiya/scanner/ui/GuideActivity.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.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
http://schemas.android.com/apk/res/android	z0/i.java
https://appservice.2363nice.com/api/	r5/d.java
http://image.kunyumobile.com/web/privacy/axscan.html	x4/b.java
http://ns.adobe.com/xap/1.0/	r1/a.java
https://toblog.ctobsnssdk.com/service/2/device_register/	a3/a.java
https://toblog.ctobsnssdk.com/service/2/app_alert_check/	a3/a.java
https://toblog.ctobsnssdk.com/service/2/app_log/	a3/a.java
https://tobapplog.ctobsnssdk.com/service/2/app_log/	a3/a.java
https://toblog.ctobsnssdk.com/service/2/profile/	a3/a.java
https://toblog.ctobsnssdk.com/service/2/log_settings/	a3/a.java
https://toblog.ctobsnssdk.com/service/2/abtest_config/	a3/a.java
https://success.ctobsnssdk.com/service/2/app_log/	a3/a.java
https://toblog-alink.ctobsnssdk.com/service/2/attribution_data	a3/a.java
https://toblog-alink.ctobsnssdk.com/service/2/alink_data	a3/a.java
https://log.snssdk.com/service/2/device_register/	a3/a.java

URL信息	Url所在文件
https://ichannel.snssdk.com/service/2/app_alert_check/	a3/a.java
https://log.snssdk.com/service/2/app_log/	a3/a.java
https://applog.snssdk.com/service/2/app_log/	a3/a.java
https://rtlog.snssdk.com/service/2/app_log/	a3/a.java
https://rtapplog.snssdk.com/service/2/app_log/	a3/a.java
https://log.snssdk.com/service/2/log_settings/	a3/a.java
https://databyterangers.com.cn	b3/p0.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.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.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.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_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.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.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.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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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。
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=js, ST=js, L=js, O=js, OU=js, CN=js
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-11-10 07:53:42+00:00
Valid To: 2121-10-17 07:53:42+00:00
Issuer: C=js, ST=js, L=js, O=js, OU=js, CN=js
Serial Number: 0x4760068e
Hash Algorithm: sha256
md5: 0974d0b62c84fe807f9fb890c0c8e812
sha1: 1aeeeef8afdbef46125de15caeaf59a3ef9ea7fe
sha256: 7fea12364a5b23a2017b53d6f8fec9d6815f458ba963e494e809073a1b59d3c4
sha512: ddb6972adcb50543393ef10d12e8f2d94816b797538e39216917c6a13b60bb07f6d615d15fb88b03c636245ecda6756d889010b043bb05dc7b94023cbc21c00e
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 7135804a3b6e1b7eea610570b1cede3f0e6ee5bb0461b9f4713d5e20f49111e4

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

加壳分析

文件列表	分析结果

<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>反虚拟机</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
possible Build.SERIAL check
network operator name check
device ID check
voice mail number check
subscriber ID check
ro.product.device check</td></tr>
<tr><td>编译器</td><td>unknown (please file detection issue!)</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>反虚拟机</td><td>Build.MANUFACTURER check
Build.TAGS check
subscriber ID check
emulator file check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>