MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

4S超级站长 1.3.8.APK

APP名称:	4S超级站长
包名:	com.lanmuda.super4s
域名线索:	20条
URL线索:	23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: 4scjzz569060.apk
文件大小: 9.23MB
MD5值: f07969162763ee5a2ff4ed1f05e0b50f
SHA1值: 415e9c781e5e13ae4767ea9c7be06b82070b854d
SHA256值: f46a8223ad2474a86e77379972bb852c763509c2beac59758e5a6b642a5c6a00

APP 信息

App名称: 4S超级站长
包名: com.lanmuda.super4s
主活动**Activity:** com.lanmuda.super4s.MainFirstActivity
安卓版本名称: 1.3.8
安卓版本: 8

域名线索

域名	是否危险域名	服务器信息
h5.xiongfenxiang.com	good	**IP:** 121.196.192.62 **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
cfg.imtt.qq.com	good	**IP:** 121.51.158.70 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map
mqqad.html5.qq.com	good	**IP:** 0.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
bjuser.jpush.cn	good	**IP:** 122.9.9.94 **所属国家:** Hong Kong **地区:** Hong Kong **城市:** Hong Kong **纬度:** 22.285521 **经度:** 114.157692 **查看地图:** Google Map

域名	是否危险域名	服务器信息
debugtbs.qq.com	good	**IP:** 175.27.9.46 **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
api.lanmudata.com	good	**IP:** 47.111.208.213 **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
debugx5.qq.com	good	**IP:** 175.27.9.46 **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
qiniu.xkxfx.com	good	没有服务器地理信息.
wup.imtt.qq.com	good	**IP:** 182.254.56.113 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map

域名	是否危险域名	服务器信息
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.105 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
log.tbs.qq.com	good	**IP:** 109.244.244.37 **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
www.qq.com	good	**IP:** 175.27.8.138 **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
182.92.20.189	good	**IP:** 182.92.20.189 **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
pms.mb.qq.com	good	**IP:** 121.51.158.70 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
tsis.jpush.cn	good	**IP:** 43.247.88.120 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
devapi.lanmudata.com	good	**IP:** 47.111.178.193 **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
mdc.html5.qq.com	good	**IP:** 175.27.9.46 **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
hydra.alibaba.com	good	**IP:** 203.119.169.227 **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
cdn.lanmudata.com	good	**IP:** 118.31.219.219 **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

URL线索

URL信息	Url所在文件
www.qq.com	com/tencent/smtt/sdk/ag.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/ag.java
http://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java

URL信息	Url所在文件
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/d.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/s.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/s.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/s.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/s.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/s.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/s.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/s.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/s.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/i.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/c/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/a/b.java
http://qiniu.xkxfx.com/	com/lanmuda/super4s/a/a/a.java
http://h5.xiongfenxiang.com	com/lanmuda/super4s/a/a/a.java

URL信息	Url所在文件
http://cdn.lanmudata.com/super4s/privacy_policy.html	com/lanmuda/super4s/view/me/b.java
http://cdn.lanmudata.com/super4s/user_agreement.html	com/lanmuda/super4s/view/me/a.java
http://devapi.lanmudata.com/	com/lanmuda/super4s/view/invitation/InvitationFragment.java
https://api.lanmudata.com/	com/lanmuda/super4s/d/c.java
http://cdn.lanmudata.com/super4s/user_agreement.html	com/lanmuda/super4s/common/dialog/b.java
http://cdn.lanmudata.com/super4s/privacy_policy.html	com/lanmuda/super4s/common/dialog/a.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ab/b.java
https://tsis.jpush.cn	cn/jiguang/ae/i.java
http://182.92.20.189:9099/	cn/jiguang/p/a.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
com.lanmuda.super4s.permission.JPUSH_MESSAGE	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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=上海, L=上海, O=4S超级站长, OU=4S超级站长, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-10-16 03:01:23+00:00
Valid To: 2129-04-22 03:01:23+00:00
Issuer: C=CN, ST=上海, L=上海, O=4S超级站长, OU=4S超级站长, CN=Unknown
Serial Number: 0x75aa34a4
Hash Algorithm: sha256
md5: dc5358e9236b6635ba1916f6f1adea40
sha1: 3b99d20873e5d7d9495b7ef3ee6d06446543e664
sha256: 46be5671f90eef6d1facff75fd0ea8d54fa4e629f6dd8c96be4916efb40c75e0
sha512: c91a9986c6a5b054cd090c86560132416cde2191cf1032d9d3ea5aa014971212d4fd56703672fbb483c68d28f67bd36ea9ab0a91963855b6e05e85b1e54b44d8
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 38b956f28054171b38adff3d8f43b8201c2be0f93fab7402c2dc15091d6614e7

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check network operator name check device ID check subscriber ID check 编译器：r8
