MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

好生意管家 V1.0.2.APK

APP名称:	好生意管家
包名:	com.xiaoyi.business
域名线索:	13条
URL线索:	13条
邮箱线索:	0条
分析日期:	2022年2月2日 20:09

文件信息

文件名: hsygj370263.apk
文件大小: 3.67MB
MD5值: 19ebe74e1c1263f72c997bf2cf8574d1
SHA1值: 07c4e8b7d817a9e57392b4653179ca81aad2ae8f
SHA256值: 6dac67c6b05627543f97ff22249be919f0e462274396fb34df2bc00fabad5ae8

APP 信息

App名称: 好生意管家
包名: com.xiaoyi.business
主活动**Activity:** com.xiaoyi.business.Activity.SplashActivity
安卓版本名称: V1.0.2
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
android.bugly.qq.com	good	**IP:** 109.244.244.137 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
aaid.umeng.com	good	IP: 111.225.159.27 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map
sj.qq.com	good	IP: 109.244.244.234 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
alogus.umeng.com	good	IP: 106.11.43.144 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
developer.umeng.com	good	IP: 59.82.29.248 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
ouplog.umeng.com	good	IP: 47.74.172.218 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
ulogs.umengcloud.com	good	IP: 106.11.40.44 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
plbslog.umeng.com	good	IP: 59.82.43.171 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
rqd.uu.qq.com	good	IP: 182.254.88.184 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
ulogs.umeng.com	good	IP: 59.82.31.151 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
pslog.umeng.com	good	IP: 59.82.31.160 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
alogsus.umeng.com	good	IP: 59.82.31.151 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
github.com	good	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://sj.qq.com/myapp/detail.htm?apkName=com.lmiot.autotool&apkCode=33	com/xiaoyi/business/Fragment/ShopFragment.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java

URL信息	Url所在文件
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultLoadReporter.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultPatchReporter.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.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.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_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.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.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=li, ST=li, L=li, O=li, OU=li, CN=li
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-10-08 02:06:09+00:00
Valid To: 2121-09-14 02:06:09+00:00
Issuer: C=li, ST=li, L=li, O=li, OU=li, CN=li
Serial Number: 0x6833c94e

Hash Algorithm: sha256
md5: 13d2e15167e1aecc2398fff4f836b65f
sha1: 451fef8c91fdb8d4d0e59acf6da3ee844dce286c
sha256: f8eedab8dc8841d11d6f8f61b32c11834a7452ebe536d2a6de0dd1a50e6adb35
sha512: 01a4435ff58acf88656675fb3810187edb6313181446ee4c91265645b79c0d886db8658b4f3077899e30fe72d820482f318237d7e6245524a3f61d7812e0d40f
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3cd5a51079979808239b2bffa00e282e1977309ac277aaaa879fbdee3d2ef512

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果

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.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check network operator name check subscriber ID check network interface name check possible ro.secure check 编译器：r8 without marker (suspicious)