MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

布谷医生 1.0.8.APK

APP名称:	布谷医生
包名:	com.bugu120.doctor
域名线索:	3条
URL线索:	5条
邮箱线索:	0条
分析日期:	2022年2月2日 17:07

文件信息

文件名: buguyisheng444192.apk
文件大小: 9.37MB
MD5值: ef94f88fe0289184086ccbc7d5199825
SHA1值: 57c58515d1df93997428970db62d323b12ced686
SHA256值: 98d80b464d66d6cc29db8f8b7c34721964911b5c74cc6b335205a0b78e319a6f

APP 信息

App名称: 布谷医生
包名: com.bugu120.doctor
主活动**Activity:** com.bugu120.doctor.ui.act.SplashActivity
安卓版本名称: 1.0.8
安卓版本: 8

域名线索

域名	是否危险域名	服务器信息
errlog.umeng.com	good	**IP:** 111.225.159.19 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

域名	是否危险域名	服务器信息
errlogos.umeng.com	good	**IP:** 47.246.110.18 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
lame.sf.net	good	**IP:** 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://lame.sf.net	lib/armeabi-v7a/libandroidlame.so
http://lame.sf.net	lib/x86_64/libandroidlame.so
http://lame.sf.net	lib/x86/libandroidlame.so
http://lame.sf.net	lib/arm64-v8a/libandroidlame.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so

URL信息	Url所在文件
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi/libcrashsdk.so

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.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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

向手机申请的权限	是否危险	类型	详细情况
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_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=zh, ST=bj, L=bj, O=bugu, OU=bugu, CN=bugu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-10-12 02:09:48+00:00
Valid To: 2119-09-19 02:09:48+00:00
Issuer: C=zh, ST=bj, L=bj, O=bugu, OU=bugu, CN=bugu
Serial Number: 0x67f4159d
Hash Algorithm: sha256
md5: 024d3ec24b2c287ede17240a9d47d79b
sha1: b22bb4c92019089350640609b38192ffa699f50e
sha256: 97e80c2ae800bb2ae748e382a4b033ea0adf2367072575ed530aaf26125cc82e
sha512: e812dc6961abd808b7cd53028d51ba3584270c7a6aa84652d0c988e8c89e3dbd69b24efaf2a72815969373dde32059e5bcfe40f07e483d509516c516141def4b
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3a7cec724ad447786c609fdb21d27938356c6c9924f4a6461c451ed290f18ad3

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
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check emulator file check possible VM check 编译器：r8

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
