MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

蕴勋在线 1.0.0.APK

APP名称:	蕴勋在线
包名:	com.bcloud.LXKXTSYC
域名线索:	27条
URL线索:	23条
邮箱线索:	0条
分析日期:	2022年1月20日 22:27

文件信息

文件名: yxzx.apk
文件大小: 3.4MB
MD5值: 1f683f3989920b18b1ad40b463c23b69
SHA1值: 2645f2bad5598e2bba27f4818eeb438814ca64d5
SHA256值: 4e8b42bc98b467da381fcf7f8181e40c56f8d2a2161543558e492c13ef29a756

APP 信息

App名称: 蕴勋在线
包名: com.bcloud.LXKXTSYC
主活动**Activity:** com.bufan.app.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

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

域名	是否危险域名	服务器信息
fusion.qq.com	good	**IP:** 121.51.36.15 **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
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
cgi.connect.qq.com	good	**IP:** 183.2.144.36 **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
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

域名	是否危险域名	服务器信息
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
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
packcheck.shanqing.com	good	没有服务器地理信息.
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
qzs.qq.com	good	**IP:** 121.51.49.57 **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
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
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
appsupport.qq.com	good	**IP:** 183.2.143.207 **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
wx.tenpay.com	good	**IP:** 182.254.88.167 **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
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
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
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
wspeed.qq.com	good	没有服务器地理信息.
packtrap.shanqing.com	good	没有服务器地理信息.
aexception.bugly.qq.com	good	**IP:** 101.226.233.161 **所属国家:** China **地区:** Shanghai **城市:** Shanghai **纬度:** 31.222219 **经度:** 121.458061 **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:** 109.244.217.35 **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
api.weixin.qq.com	good	**IP:** 109.244.145.152 **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
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
soft.tbs.imtt.qq.com	good	**IP:** 182.254.59.187 **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
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
openmobile.qq.com	good	**IP:** 113.96.208.233 **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

URL线索

URL信息	Url所在文件
http://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/CrashReport.java

URL信息	Url所在文件
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
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://aexception.bugly.qq.com:8012/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.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
www.qq.com	com/tencent/smtt/sdk/i.java
http://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/i.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java

URL信息	Url所在文件
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.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/d.java
https://wx.tenpay.com	e/a/f/b/b.java
https://wx.tenpay.com	e/a/f/b/a.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	e/a/d/c.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s	e/a/d/c.java
https://huatuocode.huatuo.qq.com	e/d/b/c.java
https://wspeed.qq.com/w.cgi	e/d/b/c.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	e/d/b/c.java

URL信息	Url所在文件
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	e/d/b/e/g.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	e/d/a/c/c.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	e/d/a/c/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	e/d/a/c/a.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	e/d/a/e/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	e/d/a/d/a.java
https://packcheck.shanqing.com/check?pack_name=%s&version_code=%s	lib/armeabi-v7a/libtbs.so
https://packtrap.shanqing.com/trap/trap.txt	lib/armeabi-v7a/libtbs.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否危险	类型	详细情况
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.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_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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.ACCESS_ALL_DOWNLOADS	未知	Unknown permission	Unknown permission from android reference
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=86, ST=fujian, L=fujian, O=bufanapp, OU=bufanapp, CN=bufanapp
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-30 10:20:54+00:00
Valid To: 2047-08-16 10:20:54+00:00
Issuer: C=86, ST=fujian, L=fujian, O=bufanapp, OU=bufanapp, CN=bufanapp
Serial Number: 0x34f1d25d

Hash Algorithm: sha256
md5: 3e803c353aa4cf3640540033224a29a9
sha1: a93eea4aef181a4108546fedb685940b5822a37c
sha256: f344bbe721f80ed8bcaae3293480b65db9496ea12d34adf3829a03d479401612
sha512: aa681063e40cf26225d68da550c10901025753ca04859cd72bb01f8865afb9fc0c0f180ec7db36348a8117808e96ad7b5a1087b15ada40f3f7f450dc3405eaca
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 3cfb29002d70cb93be5e1023b4fb42cc172fadac536e5ef76d76f57340f5bac3

Exodus威胁情报

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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent://,

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>反虚拟机</td><td>Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check subscriber ID check possible ro.secure check emulator file check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>
