MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

众雇宝 1.0.9.APK

APP名称:	众雇宝
包名:	com.dcloud.TRFZEGROF
域名线索:	32条
URL线索:	26条
邮箱线索:	0条
分析日期:	2022年2月2日 14:59

文件信息

文件名: zhonggubao.apk
文件大小: 3.6MB
MD5值: 3db98eec5a336cab7ba1a4af7674ba33
SHA1值: 886f4b4227905a4562f94127c11a84194a507edf
SHA256值: d6f598ffccec2f403bd750041acbe2303e8926c10e88668b26c10f3ecf206173

APP 信息

App名称: 众雇宝
包名: com.dcloud.TRFZEGROF
主活动**Activity:** com.bufan.app.SplashActivity
安卓版本名称: 1.0.9
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
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

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
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.60 **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
sdk.open.lbs.igexin.com	good	**IP:** 121.52.255.89 **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
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

域名	是否危险域名	服务器信息
wx.tenpay.com	good	**IP:** 182.254.88.166 **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
wspeed.qq.com	good	没有服务器地理信息.
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
api.weixin.qq.com	good	**IP:** 81.69.216.43 **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
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

域名	是否危险域名	服务器信息
s-gt.getui.com	good	**IP:** 183.131.7.106 **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
appsupport.qq.com	good	**IP:** 183.2.144.86 **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
packcheck.shanqing.com	good	没有服务器地理信息.
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 **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:** 175.24.219.72 **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

域名	是否危险域名	服务器信息
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
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
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
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
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
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
huatuocode.huatuo.qq.com	good	没有服务器地理信息.
c-hzgt2.getui.com	good	**IP:** 183.131.7.107 **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
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
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
packtrap.shanqing.com	good	没有服务器地理信息.
sdk.open.phone.igexin.com	good	**IP:** 124.160.127.216 **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
qzs.qq.com	good	**IP:** 182.254.48.158 **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
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
d.gt.igexin.com	good	**IP:** 124.160.124.197 **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

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
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://d.gt.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://s-gt.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://bi.	com/igexin/push/config/p.java
http://config.	com/igexin/push/config/p.java

URL信息	Url所在文件
http://stat.	com/igexin/push/config/p.java
http://log.	com/igexin/push/config/p.java
http://lbs.	com/igexin/push/config/p.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
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

URL信息	Url所在文件
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
https://packcheck.shanqing.com/check?pack_name=%s&version_code=%s	lib/x86/libtbs.so
https://packtrap.shanqing.com/trap/trap.txt	lib/x86/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
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

向手机申请的权限	是否危险	类型	详细情况
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
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

向手机申请的权限	是否危险	类型	详细情况
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
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
getui.permission.GetuiService.com.dcloud.TRFZEGROF	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed

v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=SH, L=SH, O=clkujp, OU=mqylxz, CN=ifnryb
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-08-13 12:04:26+00:00
Valid To: 2030-08-11 12:04:26+00:00
Issuer: C=CN, ST=SH, L=SH, O=clkujp, OU=mqylxz, CN=ifnryb
Serial Number: 0x1a251bf5
Hash Algorithm: sha256
md5: e2764a175793e2f1ce91eea103fcf6db
sha1: 9efd3c89b601702fce394411d24150c6934091de
sha256: 43925166cfc414222224ee206fd649ee80952a5f2c04187d8e49097fbae42b32
sha512: 13a7984f13b8ac50cbbe9f9a73e7abd960bb4054b031431d1298eac6b858af60e4894600953ee2382aa84a1391f531e64e538ba87e6f1561516954bd3b31d258
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 034570fdc48ec3b8e49f13305fa49181a4e9c0e1570b2075d64252f6955bf312

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.bufan.app.SplashActivity	Schemes: bufanapp12345://,

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101844352://,

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.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check Build.TAGS check SIM operator check subscriber ID check possible ro.secure check emulator file check 编译器: r8