MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

蜂享未来 1.0.0.APK

APP名称:	蜂享未来
包名:	com.dcloud.CDMKWQC
域名线索:	33条
URL线索:	30条
邮箱线索:	0条
分析日期:	2022年1月22日 17:43

文件信息

文件名: fxwl.apk
文件大小: 4.78MB
MD5值: 665709679a5d36654962aaf2864f0cec
SHA1值: 64c3428e0893a996e01114d8539495f10f11e003
SHA256值: 91ef84df3cd01cd78fa20922bb03ff1c8bde2c4a8ec80e67218dec29160653ef

APP 信息

App名称: 蜂享未来
包名: com.dcloud.CDMKWQC
主活动**Activity:** com.bufan.app.MainActivity
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
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
wspeed.qq.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
ulogs.umengcloud.com	good	IP: 106.11.86.76 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
ulogs.umeng.com	good	IP: 106.11.43.142 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
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
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

域名	是否危险域名	服务器信息
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
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
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
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

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
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
packtrap.shanqing.com	good	没有服务器地理信息.
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
tsis.jpush.cn	good	IP: 43.247.88.119 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

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.
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
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
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
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
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
alogus.umeng.com	good	IP: 59.82.29.246 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
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
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
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
cmnsguider.yunos.com	good	**IP:** 203.119.169.69 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
ce3e75d5.jpush.cn	good	**IP:** 183.232.58.243 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

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
alogsus.umeng.com	good	IP: 106.11.86.69 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: 182.254.52.119 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
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

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

URL线索

URL信息	Url所在文件
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.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://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java

URL信息	Url所在文件
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.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
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

URL信息	Url所在文件
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://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/ai/b.java
https://tsis.jpush.cn	cn/jiguang/ao/i.java
https://ce3e75d5.jpush.cn/wi/cjc4sa	cn/jiguang/aj/d.java
http://182.92.20.189:9099/	cn/jiguang/r/a.java
https://wx.tenpay.com	f/a/f/b/b.java
https://wx.tenpay.com	f/a/f/b/a.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	f/a/d/e.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s	f/a/d/e.java
https://huatuocode.huatuo.qq.com	f/d/b/c.java
https://wspeed.qq.com/w.cgi	f/d/b/c.java

URL信息	Url所在文件
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	f/d/b/c.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	f/d/b/e/e.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	f/d/a/c/c.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	f/d/a/c/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	f/d/a/c/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	f/d/a/d/a.java
https://packcheck_dbq.shanqing.com/check?pack_name=%s&version_code=%s	lib/armeabi-v7a/libtbs.so
https://packtrap.shanqing.com/trap/trap_dbq.txt	lib/armeabi-v7a/libtbs.so
https://packcheck_dbq.shanqing.com/check?pack_name=%s&version_code=%s	lib/x86/libtbs.so
https://packtrap.shanqing.com/trap/trap_dbq.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
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

向手机申请的权限	是否危险	类型	详细情况
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
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
com.dcloud.CDMKWQC.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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

向手机申请的权限	是否危险	类型	详细情况
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
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.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: O=(android-name-499789292898353152), OU=(ou)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-04-16 10:54:29+00:00
Valid To: 2047-09-02 10:54:29+00:00
Issuer: O=(android-name-499789292898353152), OU=(ou)

Serial Number: 0x34f4344d
Hash Algorithm: sha256
md5: cbeb311b0a00ceab9497ce3853566eee
sha1: 44dd61224b8cce8746c23d61d9a9b8f2911f0476
sha256: f2d4afb27bf6e9691cc79caf6bf4f901216f08f38ce3c2c29e4f42a0e17d8ca3
sha512: f7150ad8eaf0a0edc916a5c319571b2b47c3ea5eb2efe6d593bbef15b7bfbb7cf3086ee38e4f65622626299267f85d6ecb68c0a5c03f0ee0e3a56150e297563e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 124331ebcd772542c47644c1004a834774bfba454cf3adc4dc16b13643465d05

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
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

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
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.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>
