MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

羊毛帝 1.3.4.APK

APP名称:	羊毛帝
包名:	com.yangmaodi.app
域名线索:	27条
URL线索:	41条
邮箱线索:	0条
分析日期:	2022年1月26日 20:26

文件信息

文件名: yangmaodi.apk
文件大小: 3.5MB
MD5值: 208c23cc393439af8c7a4a696f6db719
SHA1值: 724ad9e6117dc976f4eab28a564589be1dfc81b0
SHA256值: c2c585a0e041be8476cbbb84f303251d1cf2b23e830ed3b9f31d9294564c586a

APP 信息

App名称: 羊毛帝
包名: com.yangmaodi.app
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.3.4
安卓版本: 13

域名线索

域名	是否危险域名	服务器信息
alog.umeng.co	good	没有服务器地理信息.
sdk.open.inc2.igexin.com	good	没有服务器地理信息.
ask.dcloud.net.cn	good	**IP:** 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map

域名	是否危险域名	服务器信息
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
pingma.qq.com	good	IP: 119.45.78.184 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: 203.119.174.133 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

域名	是否危险域名	服务器信息
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
m3w.cn	good	**IP:** 124.239.227.208 **所属国家:** China **地区:** Hebei **城市:** Langfang **纬度:** 39.509720 **经度:** 116.694717 **查看地图:** Google Map
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **查看地图:** Google Map
stream.dcloud.net.cn	good	**IP:** 118.31.188.88 **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
c-hzgt2.getui.com	good	IP: 183.131.7.108 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
service.dcloud.net.cn	good	IP: 120.26.1.80 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
schemas.android.com	good	没有服务器地理信息.
d.gt.igexin.com	good	IP: 183.134.98.71 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
sdk.open.phone.igexin.com	good	IP: 124.160.127.196 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
alog.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
log.umsns.com	good	IP: 59.82.31.95 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
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
update.dcloud.net.cn	good	IP: 121.51.175.120 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
streamapp.sinaapp.com	good	**IP:** 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 查看地图: Google Map
www.dcloud.io	good	**IP:** 124.95.157.146 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map
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
mta.oa.com	good	**IP:** 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sdk.open.amp.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
mta.qq.com	good	**IP:** 220.194.87.235 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://alogus.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://log.umsns.com/share/api/	com/umeng/analytics/social/f.java
http://log.umsns.com/	com/umeng/analytics/social/e.java

URL信息	Url所在文件
http://log.umsns.com/share/api/	com/umeng/analytics/social/e.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/sdk/diffdev/a/f.java
http://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/sdk/diffdev/a/d.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
http://bi.	com/igexin/push/config/n.java
http://config.	com/igexin/push/config/n.java
http://stat.	com/igexin/push/config/n.java
http://log.	com/igexin/push/config/n.java
http://amp.	com/igexin/push/config/n.java
http://lbs.	com/igexin/push/config/n.java
http://inc.	com/igexin/push/config/n.java
http://sdk.open.amp.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java

URL信息	Url所在文件
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.inc2.igexin.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://sdk.open.phone.igexin.com/api/addr.htm	com/igexin/push/extension/distribution/gbd/d/b.java
http://d.gt.igexin.com/api.htm	com/igexin/push/extension/distribution/basic/h/c.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://m3w.cn/sd/reg	io/dcloud/appstream/SideBar.java
http://m3w.cn/s/	io/dcloud/appstream/share/Streamapp_Share.java
http://ask.dcloud.net.cn/article/283	io/dcloud/feature/b.java

URL信息	Url所在文件
https://service.dcloud.net.cn/advert/splash	io/dcloud/feature/ad/a/a.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/common/b/a.java
https://service.dcloud.net.cn/collect/plusapp/action?	io/dcloud/common/util/TestUtil.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	io/dcloud/common/a/d.java
https://service.dcloud.net.cn/collect/plusapp/startup	io/dcloud/common/a/d.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
http://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java

URL信息	Url所在文件
http://update.dcloud.net.cn/apps/	io/dcloud/common/constant/IntentConst.java
http://streamapp.sinaapp.com	io/dcloud/streamdownload/utils/CommitPointData.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

向手机申请的权限	是否危险	类型	详细情况
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
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码

向手机申请的权限	是否危险	类型	详细情况
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.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
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.android.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcherL.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.qiku.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章

向手机申请的权限	是否危险	类型	详细情况
com.zte.mifavor.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lenovo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.google.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher3.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
org.adw.launcher_donut.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.nd.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.android.mylauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ztemt.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.gionee.amisystem.permission.READ_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
getui.permission.GetuiService.com.yangmaodi.app	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=beijing, L=beijing, O=ymd, OU=ymd, CN=ymd
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-07-02 07:50:40+00:00
Valid To: 2045-11-17 07:50:40+00:00
Issuer: C=CN, ST=beijing, L=beijing, O=ymd, OU=ymd, CN=ymd
Serial Number: 0x3f2a0b04

Hash Algorithm: sha256
md5: a9b3ee45ef517819991bc573a25b289b
sha1: 6ebbf1235be258e81df074a293d7c7a85310b6c4
sha256: c869aa51e8c70ad078e486c5bef7db6381a72c30bbc3c7b5d59ff947cfeb3df1
sha512: b65bb717a019349291ccb8bdc76f1e4771f49ba89568115b7e3458a8a726ea6670c4a8f6b5885dd2abe7987da9a53291f991db7588ef6be9b3b2816601249629

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
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	<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.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check possible VM check</td></tr><tr><td>编译器</td><td>dx</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>assets/tcore.jar!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>subscriber ID check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
