MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

波相牧场 1.0.0.APK

APP名称:	波相牧场
包名:	com.dcloud.XRSQPIOKI
域名线索:	53条
URL线索:	40条
邮箱线索:	2条
分析日期:	2022年1月22日 17:43

文件信息

文件名: bxmc.apk
文件大小: 5.17MB
MD5值: 8521ca68ce09e762ea85bc72206f4690
SHA1值: d1944150743e94c896094036e30589964fe9557e
SHA256值: 4dc40884e9ba9bccce0fae9baa4df78922c1b3227c3ba319a2afdb3a9c54cc19

APP 信息

App名称: 波相牧场
包名: com.dcloud.XRSQPIOKI
主活动**Activity:** com.yipinapp.hello.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
fontawesome.io	good	**IP:** 54.198.239.119 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 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: 183.134.98.68 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
wup.imtt.qq.com	good	IP: 182.254.57.56 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.
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
mta.qq.com	good	IP: 125.39.171.64 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

域名	是否危险域名	服务器信息
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
scripts.sil.org	good	**IP:** 104.22.11.254 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
ulogs.umeng.com	good	**IP:** 59.82.31.151 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
docs.google.com	good	**IP:** 104.244.43.52 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446 查看地图: Google Map

域名	是否危险域名	服务器信息
materialdesignicons.com	good	**IP:** 34.234.179.93 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488 查看地图: Google Map
ouplog.umeng.com	good	**IP:** 47.74.172.6 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
developer.umeng.com	good	**IP:** 59.82.29.249 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: 183.131.7.107 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
mikepenz.com	good	IP: 104.21.27.65 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
paolorotolo.github.io	good	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708 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
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
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
fontawesome.com	good	**IP:** 104.18.23.52 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
100.69.168.33	good	**IP:** 100.69.168.33 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
agoodm.m.taobao.com	good	**IP:** 59.82.31.115 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
agoodm.wapa.taobao.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
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

域名	是否危险域名	服务器信息
tsis.jpush.cn	good	IP: 183.232.58.227 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
huatuocode.huatuo.qq.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
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: 122.9.15.248 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

域名	是否危险域名	服务器信息
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
github.com	good	**IP:** 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903 查看地图: Google Map
qzs.qq.com	good	**IP:** 121.51.82.80 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
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
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
alogus.umeng.com	good	**IP:** 59.82.31.151 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
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
plbslog.umeng.com	good	**IP:** 106.11.223.204 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
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
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
xmlpull.org	good	**IP:** 74.50.62.60 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
cmnsguider.yunos.com	good	**IP:** 203.119.169.176 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
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
adash.man.aliyuncs.com	good	IP: 59.82.40.77 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: 183.131.7.102 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
alogsus.umeng.com	good	IP: 106.11.86.78 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
100.69.165.28	good	**IP:** 100.69.165.28 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000 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
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
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
http://scripts.sil.org/OFL	com/mikepenz/iconics/typeface/library/fontawesome/FontAwesome.java
https://fontawesome.com/	com/mikepenz/iconics/typeface/library/fontawesome/FontAwesome.java
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
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
http://pingma.qq.com:80/mstat/report	com/tencent/stat/StatConfig.java
http://mta.qq.com/	com/tencent/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/stat/StatServiceImpl.java

URL信息	Url所在文件
http://mta.qq.com/mta/api/ctr_feedback/add_feedback	com/tencent/stat/d.java
http://mta.qq.com/mta/api/ctr_feedback/get_feedback	com/tencent/stat/d.java
http://mta.qq.com/mta/api/ctr_feedback/reply_feedback	com/tencent/stat/d.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

URL信息	Url所在文件
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://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b.java
https://wspeed.qq.com/w.cgi	com/tencent/open/b.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	com/tencent/open/b.java
http://docs.google.com/gview?embedded=true&url=	com/thefinestartist/finestwebview/FinestWebViewActivity.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

URL信息	Url所在文件
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
http://stat.	com/igexin/push/config/p.java
http://log.	com/igexin/push/config/p.java
http://lbs.	com/igexin/push/config/p.java
http://schemas.android.com/apk/res/android	b/h/b/c/g.java
http://182.92.20.189:9099/	cn/jiguang/o/c.java
https://tsis.jpush.cn	cn/jiguang/ad/i.java
https://bjuser.jpush.cn/v1/appawake/status	cn/jiguang/aa/b.java
http://xmlpull.org/v1/doc/features.html#indent-output	e/k/a/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	e/k/a/b/a/a.java
http://100.69.165.28/agoo/report	e/l/a/m/a.java
http://agoodm.m.taobao.com/agoo/report	e/l/a/m/a.java

URL信息	Url所在文件
http://agoodm.wapa.taobao.com/agoo/report	e/l/a/m/a.java
http://100.69.168.33/agoo/report	e/l/a/m/a.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	e/m/c/b/g.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	e/m/a/c/a.java
https://openmobile.qq.com/oauth2.0/m_authorize?	e/m/a/c/a.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	e/m/a/e/b.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	e/m/a/e/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	e/m/a/d/a.java
http://adash.man.aliyuncs.com:80/man/api?ak=23356390&s=	e/a/a/a/b/a.java
http://mikepenz.com/	Android String Resource
https://github.com/mikepenz/Android-Iconics	Android String Resource
https://materialdesignicons.com/	Android String Resource
http://fontawesome.io/icons/	Android String Resource
https://github.com/FortAwesome/Font-Awesome	Android String Resource
http://paolorotolo.github.io/	Android String Resource

URL信息	Url所在文件

https://github.com/PaoloRotolo/AppIntro	Android String Resource

邮箱线索

邮箱地址	所在文件
sal@fap2fx.qpsjx	e/q/a/k.java
ctwap@mycdma.cn	e/m/b/a/b.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.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.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.CAMERA2	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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_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_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

向手机申请的权限	是否危险	类型	详细情况
android.permission.ACCESS_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ASSISTED_GPS	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_LOCATION	未知	Unknown permission	Unknown permission from android reference
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_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
com.dcloud.XRSQPIOKI.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_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
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
getui.permission.GetuiService.com.dcloud.XRSQPIOKI	未知	Unknown permission	Unknown permission from android reference
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_INSTALL	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN, ST=Chengdu, L=Chengdu, O=app861862, OU=app861862, CN=app861862
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-20 12:58:31+00:00
Valid To: 2074-12-22 12:58:31+00:00
Issuer: C=CN, ST=Chengdu, L=Chengdu, O=app861862, OU=app861862, CN=app861862

Serial Number: 0x31ffa2de
Hash Algorithm: sha256
md5: 4f3ce732b53c028995bd5ca587fcd82c
sha1: 2a7d134fdf51a3e5924820e7a920b59efd734ac7
sha256: 63075e1d03bec73841c3eea30d26af6e32230df35e6149a11d768a1a10009fa9
sha512: 2ab5657cb14e4f601d4ac33954c40534eed978751ffb23e6cb7df6ca9e6068afc78d422f5bbfb7cc2369e2ee124fd3b0dc365cf80bfd75ee1968cdef49a510b9
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 640556042690cbd31dc3c68cf5ca5accc851af03a5022c9a667834e99bfb848a

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
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

硬编码敏感信息

可能的敏感信息
"library_AndroidIconics_author" : "Mike Penz"
"library_AndroidIconics_authorWebsite" : "http://mikepenz.com/"
"library_FontAwesome_author" : "Dave Gandy"

可能的敏感信息
"library_FontAwesome_authorWebsite" : "https://materialdesignicons.com/"
"library_appintro_author" : "Paolo Rotolo"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"
"library_appintro_author" : "Paolo Rotolo"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"

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

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>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>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>
</td></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>
