MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

红包先森 2.0.1.APK

APP名称:	红包先森
包名:	cn.ydzhuan.android.mainapp
域名线索:	24条
URL线索:	50条
邮箱线索:	0条
分析日期:	2022年2月2日 11:50

文件信息

文件名: hongbaoxs.apk
文件大小: 5.09MB
MD5值: fa6d22608f902094e03018ba58e044d7
SHA1值: 42df0852670147899796493e2f32203272a72412
SHA256值: aba18e837d060a92d6233918f4a12409b21ee40d95c4bd4c256cac474d50c548

APP 信息

App名称: 红包先森
包名: cn.ydzhuan.android.mainapp
主活动**Activity:** cn.ydzhuan.android.mainapp.ui.TestActivity
安卓版本名称: 2.0.1
安卓版本: 21

域名线索

域名	是否危险域名	服务器信息
c.isdspeed.qq.com	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
mta.qq.com	good	IP: 111.161.14.94 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
statsonline.pushct.baidu.com	good	IP: 110.242.69.56 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
www.pgyer.com	good	IP: 203.107.44.30 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
www.baidu.com	good	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 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
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
lbsonline.pushct.baidu.com	good	IP: 110.242.69.54 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 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

域名	是否危险域名	服务器信息
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
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
alog.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
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
api.tuisong.baidu.com	good	IP: 110.242.69.51 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
log.umsns.com	good	IP: 59.82.31.209 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
m.baidu.com	good	IP: 110.242.68.9 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280 查看地图: Google Map
alog.umeng.co	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
cgi.connect.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
qzs.qq.com	good	IP: 182.254.48.164 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
120.24.83.14	good	IP: 120.24.83.14 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
api.hongbxs.com	good	没有服务器地理信息.
hack.tuisong.baidu.com	good	IP: 61.135.185.191 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://www.pgyer.com/	com/pgyersdk/update/PgyUpdateManager.java
http://www.pgyer.com/apiv1/feedback/add	com/pgyersdk/feedback/PgyFeedback.java
http://www.pgyer.com/	com/pgyersdk/crash/PgyCrashManager.java
http://www.pgyer.com/apiv1/crash/add	com/pgyersdk/crash/PgyCrashManager.java
http://www.pgyer.com/apiv1/crash/add	com/pgyersdk/crash/a.java
http://www.pgyer.com/apiv1/update/check	com/pgyersdk/tasks/a.java
http://www.pgyer.com/apiv1/sdkstat/install	com/pgyersdk/api/b.java
http://www.pgyer.com/apiv1/sdkstat/launch	com/pgyersdk/api/c.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
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

URL信息	Url所在文件
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://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1$s&from=%2$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
http://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statis	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/common/BaseApi.java
https://openmobile.qq.com/	com/tencent/connect/common/Constants.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApiIml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApiIml.java

URL信息	Url所在文件
http://qzs.qq.com	com/tencent/open/SocialApiIml.java
http://c.isdspeed.qq.com/code.cgi	com/tencent/open/b/d.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utils/e.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://m.baidu.com	com/baidu/android/pushservice/i.java
https://api.tuisong.baidu.com/rest/3.0/clientfile/updatesdkconfig	com/baidu/android/pushservice/config/ModeConfig.java
www.baidu.com	com/baidu/android/pushservice/util/v.java
https://hack.tuisong.baidu.com/statistics/msg_ack	com/baidu/android/pushservice/util/g.java
https://hack.tuisong.baidu.com/statistics/xiaomi/msg_ack	com/baidu/android/pushservice/util/g.java
https://hack.tuisong.baidu.com/statistics/msg_action	com/baidu/android/pushservice/util/g.java
https://hack.tuisong.baidu.com/statistics/xiaomi/msg_action	com/baidu/android/pushservice/util/g.java
http://api.tuisong.baidu.com/rest/3.0/clientad/update_ad_status	com/baidu/android/pushservice/util/a.java
https://statsonline.pushct.baidu.com/pushlog_special	com/baidu/android/pushservice/i/s.java

URL信息	Url所在文件
https://lbsonline.pushct.baidu.com/lbsupload	com/baidu/android/pushservice/i/j.java
http://api.tuisong.baidu.com/rest/3.0/oem/upload_unbind_oem	com/baidu/android/pushservice/message/a/e.java
http://api.hongbxs.com/api/android/v1/count/shareOk	cn/ydzhuan/android/mainapp/base/ZKBaseActivity.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/ydzhuan/android/mainapp/base/ZKBaseActivity.java
http://api.hongbxs.com/api/android/v1/task/giveup	cn/ydzhuan/android/mainapp/ui/MainFragment.java
http://api.hongbxs.com/api/android/v1/limitedTask/grab	cn/ydzhuan/android/mainapp/ui/MainFragment.java
http://api.hongbxs.com/api/android/v1/screenshotsTask/detail	cn/ydzhuan/android/mainapp/ui/PicTaskInforActivity.java
http://api.hongbxs.com/api/android/v1/screenshotsTask/detail	cn/ydzhuan/android/mainapp/ui/PicTaskGalleryAty.java
http://api.hongbxs.com/api/android/v1/signTask/detail	cn/ydzhuan/android/mainapp/ui/SignTaskInforActivity.java
http://api.hongbxs.com/api/android/v1/task/giveup	cn/ydzhuan/android/mainapp/ui/SignTaskInforActivity.java
http://api.hongbxs.com/api/android/v1/user/apps	cn/ydzhuan/android/mainapp/ui/MainActivityNew.java
http://api.hongbxs.com/api/android/v1/user/updateClientPush	cn/ydzhuan/android/mainapp/ui/MainActivityNew.java
http://api.hongbxs.com/api/android/v1/count/pushOk	cn/ydzhuan/android/mainapp/ui/MainActivityNew.java
http://api.hongbxs.com/api/android/v1/user/refreshToken	cn/ydzhuan/android/mainapp/ui/MainActivityNew.java
http://api.hongbxs.com/api/android/v1/screenshotsTask/detail	cn/ydzhuan/android/mainapp/ui/PicTaskWebShotAty.java

URL信息	Url所在文件
http://api.hongbxs.com/api/android/v1/limitedTask/detail	cn/ydzhuan/android/mainapp/ui/PlayTaskDetailActivity.java
http://api.hongbxs.com/api/android/v1/task/giveup	cn/ydzhuan/android/mainapp/ui/PlayTaskDetailActivity.java
http://api.hongbxs.com/api/android/v1/limitedTask/lst	cn/ydzhuan/android/mainapp/ui/TaskListActivity.java
http://api.hongbxs.com/api/android/v1/signTask/lst	cn/ydzhuan/android/mainapp/ui/TaskListActivity.java
http://api.hongbxs.com/api/android/v1/screenshotsTask/lst	cn/ydzhuan/android/mainapp/ui/TaskListActivity.java
http://api.hongbxs.com/api/android/v1/task/giveup	cn/ydzhuan/android/mainapp/ui/TaskListActivity.java
http://api.hongbxs.com/api/android/v1/user/checkPCode	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/bindwechat	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/cash/application	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/cash	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/cash/logLst	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/cash/ways	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/home	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/app/welcome	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/fundLogs	cn/ydzhuan/android/mainapp/engine/Global.java

URL信息	Url所在文件
http://api.hongbxs.com/api/android/v1/invitation	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/invitation/levelLst	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/invitation/logLst	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/invitation/reward	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/superTask/info	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/superTask/lst	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/home/bindInvite	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/task/home	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/info	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/msgs	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/getPCode	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/updateAvatar	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/user/updateNickName	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/superTask/log	cn/ydzhuan/android/mainapp/engine/Global.java

URL信息	Url所在文件
http://api.hongbxs.com/api/android/v1/	cn/ydzhuan/android/mainapp/engine/Global.java
http://120.24.83.14:8890/	cn/ydzhuan/android/mainapp/engine/Global.java
http://api.hongbxs.com/api/android/v1/signTask/grab	cn/ydzhuan/android/mainapp/adapter/ViewSignTaskListAdapter.java
http://api.hongbxs.com/api/android/v1/limitedTask/grab	cn/ydzhuan/android/mainapp/adapter/ViewDownTaskListAdapter.java
http://api.hongbxs.com/api/android/v1/screenshotsTask/upload	cn/ydzhuan/android/mainapp/view/ViewShotSuccess.java
http://api.hongbxs.com/api/android/v1/user/login	cn/ydzhuan/android/mainapp/utils/LoginUtils.java
http://api.hongbxs.com/api/android/v1/app/versionCount	cn/ydzhuan/android/mainapp/utils/AppUpdateUtil.java
http://120.24.83.14:8891/w/link/100315	Android String Resource

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.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

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.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。

向手机申请的权限	是否危险	类型	详细情况
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.ACCESS_DOWNLOAD_MANAGER	未知	Unknown permission	Unknown permission from android reference
android.permission.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
android.permission.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.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
baidu.push.permission.WRITE_PUSHINFOPROVIDER.cn.ydzhuan.android.mainapp	未知	Unknown permission	Unknown permission from android reference
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

签名证书

APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=GuangDong, L=GuangZhou, O=广州竹叶禾子网络科技有限公司, OU=广州竹叶禾子网络科技有限公司, CN=广州竹叶禾子网络科技有限公司
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-08-03 07:16:21+00:00
Valid To: 2042-07-28 07:16:21+00:00
Issuer: C=cn, ST=GuangDong, L=GuangZhou, O=广州竹叶禾子网络科技有限公司, OU=广州竹叶禾子网络科技有限公司, CN=广州竹叶禾子网络科技有限公司
Serial Number: 0x68061c62
Hash Algorithm: sha256
md5: 4dd06311d9e1a949806f42d701042ed9
sha1: c594987b492457963f9c66a9a03055cc516ef7cd
sha256: 8513e1b667217f357f2380782a91f5c31ce6ec79afb95133f2246179263078e0
sha512: 76fce20486f51ba386c241322a2f46353507a40a6720b0dc663c52e85032de76750bd7235d0a90587b03caf24e735a74c3952ec6901891fb9731ba182cfe5537

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

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1106268231://,

加壳分析

<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.BOARD check
possible Build.SERIAL check
SIM operator check
network operator name check
subscriber ID check
possible VM check</td></tr>
<tr><td>编译器</td><td>dx (possible dexmerge)</td></tr>
<tr><td>Manipulator Found</td><td>dexmerge</td></tr>
</table>
</td></tr>
</table>
