MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

有成报销 1.0.2.APK

APP名称:	有成报销
包名:	com.raycloud.yiqibao
域名线索:	28条
URL线索:	24条
邮箱线索:	1条
分析日期:	2022年2月3日 13:14

文件信息

文件名: youchengbaoxiao558628.apk
文件大小: 4.29MB
MD5值: b89810c17d0c4d104a872b1f694211ff
SHA1值: 60e958ddfd4bac30a3885c27ff8a34e46af66f49
SHA256值: 6cd9d16ea0d829001c869336fa95d841435b3b365bb6b7fa0049010a5d3cc76e

APP 信息

App名称: 有成报销
包名: com.raycloud.yiqibao
主活动**Activity:** com.raycloud.erp.StartUpActivity
安卓版本名称: 1.0.2
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
yiqbmobile.ycy-inc.cn	good	**IP:** 47.92.241.85 **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
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
assispda.superboss.cc	good	**IP:** 47.92.9.212 **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
yiqbmobile.superboss.cc	good	**IP:** 39.99.202.136 **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
restsdk.amap.com	good	**IP:** 106.11.43.113 **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
apilocate.amap.com	good	**IP:** 59.82.60.15 **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
dualstack-a.apilocate.amap.com	good	**IP:** 106.11.40.50 **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
oss-cn-.aliyuncs.comor	good	没有服务器地理信息.
astat.bugly.cros.wr.pvp.net	good	**IP:** 170.106.135.32 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.774929 **经度:** -122.419418 **查看地图:** Google Map
dingcwstatic.superboss.cc	good	**IP:** 39.99.218.176 **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
android.bugly.qq.com	good	**IP:** 109.244.244.137 **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
lbs.amap.com	good	**IP:** 59.82.31.99 **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
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
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
dualstack-arestapi.amap.com	good	**IP:** 39.98.22.142 **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
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
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
log.tbs.qq.com	good	**IP:** 109.244.244.32 **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
abroad.apilocate.amap.com	good	**IP:** 59.82.39.53 **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
cgicol.amap.com	good	**IP:** 59.82.31.100 **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
tbsrecovery.imtt.qq.com	good	**IP:** 109.244.244.237 **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
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

域名	是否危险域名	服务器信息
oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.248 **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
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
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
soft.tbs.imtt.qq.com	good	**IP:** 121.51.175.84 **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
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
image.cnamedomain.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://assispda.superboss.cc	com/raycloud/erp/WebArkApplication.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cc.java
http://restsdk.amap.com	com/loc/s.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/ef.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/ef.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/l.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/l.java

URL信息	Url所在文件
http://apilocate.amap.com/mobile/binary	com/loc/ek.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ed.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/eo.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
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://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
http://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
www.qq.com	com/tencent/smtt/sdk/l.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.java

URL信息	Url所在文件
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000	com/tencent/smtt/sdk/WebView.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/m.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/m.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/m.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/m.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/m.java

URL信息	Url所在文件
https://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
https://ip.	e/b/a/a/a/e.java
http://oss-cn-****.aliyuncs.com',or	e/b/a/a/a/e.java
http://image.cnamedomain.com'!	e/b/a/a/a/e.java
http://oss-cn-hangzhou.aliyuncs.com	e/g/a/a.java
https://dingcwstatic.superboss.cc/yiqibao/privacy.html	Android String Resource
https://yiqbmobile.superboss.cc/index.xhtml	Android String Resource
http://yiqbmobile.ycy-inc.cn/index.xhtml	Android String Resource

邮箱线索

邮箱地址	所在文件
6h@fo.lwft w9oi_2nhels4u@dlilycclglhl.5jlcg_bqh yay@y.u5vcghyy	lib/armeabi-v7a/libiconv.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_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
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=CN

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-09-10 07:52:28+00:00
Valid To: 2046-09-04 07:52:28+00:00
Issuer: C=CN
Serial Number: 0x7cf4dde9
Hash Algorithm: sha256
md5: 9e0b7001d3a40372ee9558c4383bc2a6
sha1: 118a2f85021c921b87d19a39300c6a480d79ea05
sha256: 0fde4ac6233490649d3bbe3de71c94f995fc598ec255e64ade2ec4f3bce88353
sha512: f9c290e49dfdab0bd3a517687fa9911946fa6cebed76c66eb38e7cf37fc0a2185616967f8be25ff2885b1846c8333e3bdcde665db9cf68ce0cae5308229d65ab
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: fec1e33936c4c707d6917591b123a0a4f0f4cb0e28e91bbefea1a5860de4ee5a

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

硬编码敏感信息

可能的敏感信息
"alimap_key" : "46b5e18cb8bc39557e790352d6a027ba"
"buglyKey" : "a6c2c7d62d"

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.raycloud.erp.BrowserOpenActivity	Schemes: https://, http://, yiqibao://, Hosts: com.raycloud.yiqibao, com.raycloud.yiqibao ,

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.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 subscriber ID check possible ro.secure check emulator file check 编译器：r8