MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

有心事树洞 1.0.APK

APP名称:	有心事树洞
包名:	com.dxngxhl.yxs
域名线索:	30条
URL线索:	55条
邮箱线索:	0条
分析日期:	2022年1月28日 23:24

文件信息

文件名: yxssd555256.apk
文件大小: 5.68MB
MD5值: 1e179e63938244e159c0d11fa87d1480
SHA1值: 6d354de6fcc4731cb34da543755ecce651787987
SHA256值: b0f34e1fa86c2379a0de40debabdaf077b43f8076862197f85c78734655062aa

APP 信息

App名称: 有心事树洞
包名: com.dxngxhl.yxs
主活动**Activity:** com.dxngxhl.yxs.hh.act.StartActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
up.sdk.mob.com	good	**IP:** 203.107.55.19 **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
loc.map.baidu.com	good	**IP:** 111.206.209.175 **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
shudong.lyhuizhuang.com	good	**IP:** 221.229.204.139 **所属国家:** China **地区:** Jiangsu **城市:** Xuzhou **纬度:** 34.266666 **经度:** 117.166664 **查看地图:** Google Map
api.data.sentinel.mob.com	good	没有服务器地理信息.
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
app.qq.com	good	**IP:** 182.254.63.77 **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
p.share.mob.com	good	没有服务器地理信息.
cgi.qplus.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
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
api.utag.mob.com	good	没有服务器地理信息.
daup.map.baidu.com	good	**IP:** 153.3.236.86 **所属国家:** China **地区:** Jiangsu **城市:** Nanjing **纬度:** 32.061668 **经度:** 118.777779 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api.map.baidu.com	good	**IP:** 111.206.208.72 **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
identify.verify.mob.com	good	**IP:** 203.107.55.19 **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
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
ofloc.map.baidu.com	good	**IP:** 111.206.209.193 **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
api.config.sentinel.mob.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
qzs.qq.com	good	**IP:** 121.51.49.44 **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:** 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
api.u.mob.com	good	没有服务器地理信息.
schemas.android.com	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
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
www.mob.com	good	**IP:** 116.62.130.46 **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
lame.sf.net	good	**IP:** 204.68.111.100 **所属国家:** United States of America **地区:** California **城市:** San Diego **纬度:** 32.799797 **经度:** -117.137047 **查看地图:** Google Map
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

域名	是否危险域名	服务器信息
itsdata.map.baidu.com	good	**IP:** 111.206.209.180 **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
init.sms.mob.com	good	**IP:** 203.107.55.19 **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
shudong.dangan.net	good	没有服务器地理信息.
api.manager.sentinel.mob.com	good	没有服务器地理信息.
graph.qq.com	good	**IP:** 121.51.23.242 **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

URL线索

URL信息	Url所在文件
http://api.u.mob.com	com/mob/MobUser.java
http://api.utag.mob.com/bdata	com/mob/commons/utag/UserTager.java
http://api.utag.mob.com/conf	com/mob/commons/utag/TagRequester.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.java
http://api.data.sentinel.mob.com	com/mob/mobapm/core/d.java
http://api.manager.sentinel.mob.com	com/mob/mobapm/core/d.java
http://api.config.sentinel.mob.com	com/mob/mobapm/core/d.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/c.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultLoadReporter.java
https://github.com/Tencent/tinker/issues	com/tencent/tinker/lib/reporter/DefaultPatchReporter.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/g/a.java
https://shudong.lyhuizhuang.com/agreement.html	com/dxngxhl/yxs/hh/act/login/LoginActivity.java
https://shudong.dangan.net/app/api.php?action=randhead?sex=	com/dxngxhl/yxs/hh/adt/HomeChildAdapter.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b/b/a/v.java
https://){1}	cn/sharesdk/framework/b/a.java
http://p.share.mob.com/tags/getTagList	cn/sharesdk/framework/authorize/f.java
https://graph.qq.com/oauth2.0/m_authorize?response_type=token&client_id=	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/oauth2.0/me	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com/user/get_simple_userinfo	cn/sharesdk/tencent/qq/c.java
https://graph.qq.com	cn/sharesdk/tencent/qq/c.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?sdkv=3.3.0.lite&display=mobile	cn/sharesdk/tencent/qq/a.java
http://app.qq.com/detail/com.tencent.mobileqq?autodownload=1&norecommend=1&rootvia=opensdk	cn/sharesdk/tencent/qq/a.java
https://api.weixin.qq.com/sns/oauth2/access_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/oauth2/refresh_token	cn/sharesdk/wechat/utils/h.java
https://api.weixin.qq.com/sns/userinfo	cn/sharesdk/wechat/utils/h.java
http://www.mob.com/about/policy	c/a/t/d.java
http://init.sms.mob.com/v3/sdk/init	c/a/s/d.java
http://identify.verify.mob.com/auth/verify/mobile	c/a/s/h/d.java

URL信息	Url所在文件
https://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	a/o/c/c/f.java
http://cgi.qplus.com/report/report	a/o/c/c/j.java
https://appsupport.qq.com/cgi-bin/appstage/mstats_batch_report	a/o/c/a/h.java
https://shudong.lyhuizhuang.com	a/a/a/e/a.java
https://shudong.lyhuizhuang.com/app/api.php/	a/a/a/e/a.java
https://shudong.dangan.net/app/api.php?action=randhead?sex=	a/a/a/a/a/f.java
https://api.map.baidu.com/sdkcs/verify	a/d/b/a/k.java
http://loc.map.baidu.com/sdk.php	a/d/c/t/g.java
https://loc.map.baidu.com/sdk.php	a/d/c/t/g.java
http://loc.map.baidu.com/indoorlocbuildinginfo.php	a/d/c/t/a.java
http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet	a/d/c/t/n/c/a.java
http://ofloc.map.baidu.com/offline_loc	a/d/c/o/k.java
http://ofloc.map.baidu.com/offline_loc	a/d/c/o/f.java
https://ofloc.map.baidu.com/offline_loc	a/d/c/o/h.java
https://ofloc.map.baidu.com/offline_loc	a/d/c/o/g.java

URL信息	Url所在文件
http://ofloc.map.baidu.com/offline_loc	a/d/c/o/c.java
http://%s/%s	a/d/c/o/c.java
http://loc.map.baidu.com/sdk_ep.php	a/d/c/l/f.java
https://daup.map.baidu.com/cltr/rcvr	a/d/c/l/g.java
https://loc.map.baidu.com/cfgs/loc/commcfgs	a/d/c/l/d.java
http://loc.map.baidu.com/sdk.php	a/d/c/l/d.java
http://loc.map.baidu.com/gpsz	a/d/c/l/a.java
http://loc.map.baidu.com/sdk.php	a/d/c/s/f.java
http://loc.map.baidu.com/sdk.php	a/d/c/s/e.java
http://loc.map.baidu.com/tcu.php	a/d/c/j/n.java
https://loc.map.baidu.com/sdk.php	a/d/c/j/k.java
https://itsdata.map.baidu.com/long-conn-gps/sdk.php	a/d/c/j/f.java
http://loc.map.baidu.com/sdk.php	a/d/c/j/u.java
https://daup.map.baidu.com/cltr/rcvr	a/d/c/j/u.java
https://loc.map.baidu.com/sdk.php	a/d/c/j/u.java

URL信息	Url所在文件
http://loc.map.baidu.com/sdk.php	a/d/c/j/h.java
http://loc.map.baidu.com/sdk.php	a/d/c/j/c.java
https://loc.map.baidu.com/sdk.php	a/d/c/j/c.java
http://loc.map.baidu.com/sdk.php	a/d/c/j/i.java
http://loc.map.baidu.com/cc.php	a/d/c/j/d.java
http://www.mob.com/policy/en	Android String Resource
http://www.mob.com	Android String Resource
http://www.mob.com/policy/zh	Android String Resource
http://lame.sf.net	lib/armeabi-v7a/libmp3lame.so
http://lame.sf.net	lib/x86/libmp3lame.so
http://lame.sf.net	lib/armeabi/libmp3lame.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.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.DELETE_CACHE_FILES	系统需要	删除其他应用程序缓存	允许应用程序删除缓存文件
android.permission.CLEAR_APP_CACHE	系统需要	删除所有应用程序缓存数据	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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_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_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.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.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_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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=yxs
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-06 06:34:23+00:00
Valid To: 2044-10-30 06:34:23+00:00
Issuer: CN=yxs
Serial Number: 0x1378bb75
Hash Algorithm: sha256
md5: 2b038ce81f7f9be4960a23edadbf707e
sha1: a48f88e65febe893789928e1f648648ac3672257
sha256: 8a10f32862656eb1b5174ddcf0c5bf1b08a1ddef732a9ccc5704c9632072e5a6
sha512: a890e4d0a20fed4653a118997c38e021cd7f06083f320cfa653c4680ea03dccfbf104dffe65ddfd42e30888571dcbfeb32176894338dd3261733ed8b6bd45dd4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 25bd49faba1622ee126a64623cc03f3c252465f81d4e5732ac20343c5be0d04d

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

硬编码敏感信息

可能的敏感信息
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"ssdk_cmcc_auth" : "手机认证服务由中国移动提供"
"ssdk_cmcc_login_one_key" : "本机号码一键登录"
"ssdk_instapaper_pwd" : "密码"
"ssdk_weibo_oauth_regiseter" : "应用授权"
"mobcommon_authorize_dialog_accept" : "同意"
"mobcommon_authorize_dialog_content" : "为了给您提供Mobservice相关产品服务，请您详细查看我们的隐私政策，详见http://www.mob.com/policy/zh。如您同意我们的隐私政策，请点击“接受”，如您不同意我们的隐私政策，请点击“拒绝”。"
"mobcommon_authorize_dialog_reject" : "拒绝"

可能的敏感信息
"mobcommon_authorize_dialog_title" : "服务授权"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"mobcommon_authorize_dialog_accept" : "Accept"
"mobcommon_authorize_dialog_content" : "In order to provide you with Mobservice, please check our service policy. For details, please click http://www.mob.com/policy/en. If you agree with our service policy, please click accept, if you do not agree with our service policy, please click reject"
"mobcommon_authorize_dialog_reject" : "Reject"
"mobcommon_authorize_dialog_title" : "Terms of Use"
"smssdk_authorize_dialog_accept" : "Agree"
"smssdk_authorize_dialog_reject" : "Disagree"
"smssdk_authorize_dialog_title" : "Terms of Use"
"ssdk_cmcc_auth" : "Provided by China Mobile"
"ssdk_cmcc_login_one_key" : "PhoneNum Login"
"ssdk_instapaper_pwd" : "Password"
"ssdk_weibo_oauth_regiseter" : "Authorization"

可能的敏感信息

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101904845://,
cn.sharesdk.tencent.qq.ReceiveActivity	Schemes: tencent101904845://,

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.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
possible ro.secure check
emulator file check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
