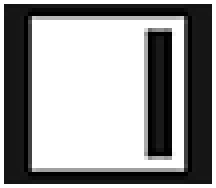
MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成



移动菜刀 1.1.1.APK

APP名称:	移动菜刀
包名:	zzu.ssx.chinesecaidao
域名线索:	17条
URL线索:	15条
邮箱线索:	0条
分析日期:	2022年1月18日 18:45

文件信息

文件名: caidao.apk
文件大小: 1.25MB
MD5值: f0700e4ee4b91613a54cbb526aa09bc5
SHA1值: 25b86b38a4b6de9b9503463427afeaf93e458a30
SHA256值: 5c2f3cd25e67228fdc85d06a6d9698e0fb4095dc4c787abaec8a0a211dca347d

APP 信息

App名称: 移动菜刀
包名: zzu.ssx.chinesecaidao
主活动**Activity:** zzu.ssx.chinesecaidao.SplashActivity
安卓版本名称: 1.1.1
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
au.umeng.co	good	没有服务器地理信息.
log.umsns.com	good	**IP:** 59.82.60.44 **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
feedback.umeng.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
qzonestyle.gtimg.cn	good	**IP:** 182.254.52.119 **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
alog.umeng.co	good	没有服务器地理信息.
alog.umeng.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
oc.umeng.co	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
ip.chinaz.com	good	**IP:** 103.205.5.186 **所属国家:** China **地区:** Jiangsu **城市:** Hutang **纬度:** 31.533331 **经度:** 119.483330 **查看地图:** Google Map
sdk.e.qq.com	good	**IP:** 58.250.137.37 **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
au.umeng.com	good	没有服务器地理信息.
aps.amap.com	good	**IP:** 59.82.60.60 **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:** 59.82.31.67 **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
lba.baidu.com	good	没有服务器地理信息.
oc.umeng.com	good	**IP:** 203.119.128.55 **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
restapi.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
apilocate.amap.com	good	**IP:** 106.11.43.81 **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

URL线索

URL信息	Url所在文件
http://au.umeng.com/api/check_app_update	com/umeng/update/b.java
http://au.umeng.co/api/check_app_update	com/umeng/update/b.java
http://alog.umeng.com/app_logs	com/umeng/analytics/a.java
http://alog.umeng.co/app_logs	com/umeng/analytics/a.java
http://oc.umeng.com/check_config_update	com/umeng/analytics/a.java
http://oc.umeng.co/check_config_update	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
http://loc.map.baidu.com/fence	com/baidu/location/au.java
http://loc.map.baidu.com/fence	com/baidu/location/a0.java
http://lba.baidu.com/	com/baidu/location/BDLocation.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/c.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/c.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/c.java

URL信息	Url所在文件
http://loc.map.baidu.com/sdk.php	com/baidu/location/c.java
http://loc.map.baidu.com/oqur.php	com/baidu/location/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/banner.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/bannerapkpop.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/open_proj/img/gdt/sdk_popup.png)	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/gridappwall.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/interstitial.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/feeds.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/feeds2.html	com/qq/e/v2/managers/setting/c.java
http://qzonestyle.gtimg.cn/qzone/biz/gdt/mob/sdk/v2/appwall.html	com/qq/e/v2/managers/setting/c.java
http://sdk.e.qq.com/activate	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/click	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/disp	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/err	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/getad	com/qq/e/v2/constants/Constants.java

URL信息	Url所在文件
http://sdk.e.qq.com/launch	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/msg	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com	com/qq/e/v2/constants/Constants.java
http://sdk.e.qq.com/conve	com/qq/e/v2/constants/Constants.java
http://restapi.amap.com/log/init	com/amap/api/location/core/a.java
http://apilocate.amap.com/mobile/binary	com/aps/n.java
http://aps.amap.com/APS/r	com/aps/n.java
http://apilocate.amap.com/mobile/binary	com/aps/j.java
http://aps.amap.com/APS/r	com/aps/j.java
http://cgicol.amap.com/collection/writedata?ver=v1.0_ali&	com/aps/j.java
http://feedback.umeng.com/feedback	u/fb/p.java
http://feedback.umeng.com/feedback/reply	u/fb/p.java
http://feedback.umeng.com/feedback/feedbacks	u/fb/p.java
http://ip.chinaz.com/?IP=	zzu/ssx/chinesecaidao/pager/pagetools.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.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.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.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.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_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.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.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_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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.ACCESS_COARSE_UPDATES	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=0371, ST=hn, L=zz, O=zz, OU=zzu, CN=qifan

Signature Algorithm: rsassa_pkcs1v15
Valid From: 2014-07-27 07:56:20+00:00
Valid To: 2114-07-03 07:56:20+00:00
Issuer: C=0371, ST=hn, L=zz, O=zz, OU=zzu, CN=qifan
Serial Number: 0x53d4b0a4
Hash Algorithm: sha1
md5: cb0ab62850a77c6ed1c376891c026f95
sha1: e708b37aba040e5c7675c385dc93d7f7e2c18a46
sha256: 856da95aa075a84a784aed46bb380416ed49367d0c30c7d7e66c4026959d019a
sha512: e1a1c1c58b1d6a86764e7b441998fabd8d538d8a127de716565cc33920bff4c02b09c93fb7972111074bf09cb6f4e04c5dc308a99f061e9a9bfa2872d36fd182

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119
Umeng Feedback		https://reports.exodus-privacy.eu.org/trackers/120

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.MODEL check
Build.MANUFACTURER check
Build.BOARD check
network operator name check
subscriber ID 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>
<tr><td>assets/gdt_plugin/gdtad.jar!classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
