MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

智慧斯马特 1.1.5.APK

APP名称:	智慧斯马特
包名:	com.qinguit.zhsmt
域名线索:	19条
URL线索:	27条
邮箱线索:	2条
分析日期:	2022年2月3日 13:32

文件信息

文件名: zhsmt.apk
文件大小: 7.93MB
MD5值: 03ab1c764ffe092c20f7eb766e10c5d5
SHA1值: b17e3c838a8cfd502d973bb3bcb2dd041de99bfd
SHA256值: 488fe5abf61dd4f85df54cc13497bd95e9511f4b84111d0907870498fca91b97

APP 信息

App名称: 智慧斯马特
包名: com.qinguit.zhsmt
主活动**Activity:** com.uzmap.pkg.LauncherUI
安卓版本名称: 1.1.5
安卓版本: 13

域名线索

域名	是否危险域名	服务器信息
api-push.meizu.com	good	**IP:** 125.94.213.129 **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
s.apicloud.com	good	没有服务器地理信息.
as.apicloud.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **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
r.apicloud.com	good	**IP:** 182.92.145.58 **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
p.apicloud.com	good	**IP:** 47.93.154.30 **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
api.u.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
norma-external-collect.meizu.com	good	**IP:** 113.106.27.98 **所属国家:** China **地区:** Guangdong **城市:** Zhongshan **纬度:** 22.520580 **经度:** 113.382317 **查看地图:** Google Map
d.apicloud.com	good	**IP:** 47.94.176.24 **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
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
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
api.utag.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
play.google.com	good	**IP:** 172.217.160.110 **所属国家:** United States of America **地区:** California **城市:** Mountain View **纬度:** 37.405991 **经度:** -122.078514 **查看地图:** Google Map
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
sdk.push.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
a.vmall.com	good	**IP:** 49.4.17.96 **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
a.apicloud.com	good	**IP:** 182.92.145.58 **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
download.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

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://www.mob.com/about/policy	com/mob/commons/dialog/d.java
http://up.sdk.mob.com	com/mob/commons/filesys/FileUploader.java

URL信息	Url所在文件
http://sdk.push.mob.com/demo/v2/push	com/mob/pushsdk/SimulateRequest.java
http://sdk.push.mob.com	com/mob/pushsdk/biz/a.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/b/c/e.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/b.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/a/b.java
http://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/a/a/b.java
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/a/a/a.java
http://a.vmall.com/app/	com/huawei/hms/update/d/f.java
https://play.google.com/store/apps/details?id=	com/huawei/hms/support/api/push/a/a/a.java
http://a.vmall.com/	com/huawei/hms/support/api/push/a/a/a.java
http://init.sms.mob.com/v3/sdk/init	cn/smssdk/utils/a.java
http://download.sdk.mob.com/e72/83d/e247e8b45bd557f70ac6dcc0cb.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/7b6/264/2c4a9fef9ffa03e5deb5973ab9.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/bbd/480/d993f23339944e4de27e4b0a12.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/3a6/b11/ba6a81f2c13fb0ba3b96d99619.png	cn/smssdk/gui/util/Const.java

URL信息	Url所在文件
http://download.sdk.mob.com/a0b/7d0/0520d3554a69ad50a3b87d1760.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/510/deb/0c0731ac543eb71311c482a2e2.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/7d7/e2b/91d898dfde6fb787ab3d926f9d.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/29f/06f/e6a941cd02e3f29465cd438d16.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/167/bc4/38197ca7950aec7020d516fbb2.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/f57/a5e/72ecd0c6ca96361c7f3bcd7144.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/e31/c6e/315fdfa6abc4b17d8c139605de.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/cc3/00e/dedc8bf1514d6c6a5e456fba74.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/f22/154/e27eaf3fc3e24047bd5d4ec3a8.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/d33/6f9/c15ee2d2f01aba51d33985e6c5.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/cc6/115/2628761069dd35867eda68fe2a.png	cn/smssdk/gui/util/Const.java
http://download.sdk.mob.com/047/a51/38cfad789e9808443d11f2f9be.png	cn/smssdk/gui/util/Const.java
https://a.apicloud.com	compile/Properties.java
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java

URL信息	Url所在文件
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java
http://www.mob.com	Android String Resource
http://lame.sf.net	lib/armeabi/libmp3lame.so

邮箱线索

邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.java
xxxx@xxxx.com	com/huawei/hms/support/api/push/a/d/a.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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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_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_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_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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
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
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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.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.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

向手机申请的权限	是否危险	类型	详细情况
android.permission.DELETE_PACKAGES	系统需要	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序
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.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_VIDEO	未知	Unknown permission	Unknown permission from android reference
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.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
com.qinguit.zhsmt.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.qinguit.zhsmt.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.qinguit.zhsmt.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.qinguit.zhsmt.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(66140223@163.com), OU=(66140223@163.com), CN=(zhsmt)
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-06-16 09:04:45+00:00
Valid To: 2120-05-23 09:04:45+00:00
Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(66140223@163.com), OU=(66140223@163.com), CN=(zhsmt)
Serial Number: 0xe51fffc
Hash Algorithm: sha256
md5: 9c1a3abd99e0dd08207c5849ab559c8d
sha1: d267e880086db8d78b9da13764d1bddf4ea35a48
sha256: 24167618d967be142f2be9a9352b34da7e6aad40d6b9c4e71ceb3f6fbca21a41

sha512: 42137a4515fe9ec692d8fdc0b425ba9ace4d8c2dbb5615be57428d9fcf3e2269d63a77a60fef6011369c134a403747bc96707be18909eb1181bbcba53312c44a
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 1b2e8695e0acdd5fc1e39048de90c7ced885337e85e8fb8312adad1dae02c8d9

Exodus威胁情报

名称	分类	URL链接
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 编译器 / dx
classes10.dex	壳列表 / 详细情况 编译器 / dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes11.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
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes12.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>
<tr><td>classes13.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>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes14.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>possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes15.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>
<tr><td>classes16.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>
<tr><td>classes17.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>
<tr><td>classes18.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>

文件列表	分析结果
classes19.dex	壳列表 / 详细情况 编译器 / dx
classes2.dex	壳列表 / 详细情况 编译器 / dx
classes20.dex	壳列表 / 详细情况 编译器 / dx
classes21.dex	壳列表 / 详细情况 编译器 / dx
classes22.dex	壳列表 / 详细情况 编译器 / dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes23.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>
<tr><td>classes24.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.MANUFACTURER check
possible Build.SERIAL check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
<tr><td>classes25.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>
<tr><td>classes26.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.MANUFACTURER check
Build.BOARD check
emulator file check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>

文件列表	分析结果
classes27.dex	壳列表 | 详细情况 编译器 | dx
classes28.dex	壳列表 | 详细情况 编译器 | dx
classes29.dex	壳列表 | 详细情况 编译器 | dx
classes3.dex	壳列表 | 详细情况 编译器 | dx
classes30.dex	壳列表 | 详细情况 编译器 | dx

文件列表	分析结果
classes31.dex	壳列表 | 详细情况 编译器 | dx
classes32.dex	壳列表 | 详细情况 编译器 | dx
classes33.dex	壳列表 | 详细情况 编译器 | dx
classes34.dex	壳列表 | 详细情况 编译器 | dx
classes35.dex	壳列表 | 详细情况 编译器 | dx

文件列表	分析结果
classes36.dex	壳列表 | 详细情况 编译器 | dx
classes37.dex	壳列表 | 详细情况 编译器 | dx
classes38.dex	壳列表 | 详细情况 编译器 | dx
classes39.dex	壳列表 | 详细情况 编译器 | dx
classes4.dex	壳列表 | 详细情况 编译器 | dx

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes40.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>
<tr><td>classes41.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>
<tr><td>classes42.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>
<tr><td>classes43.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>possible Build.SERIAL check</td></tr><tr><td>编译器</td><td>dx</td></tr></table></td></tr>
<tr><td>classes44.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>

文件列表	分析结果
classes5.dex	壳列表 / 详细情况 编译器 / dx
classes6.dex	壳列表 / 详细情况 编译器 / dx
classes7.dex	壳列表 / 详细情况 编译器 / dx
classes8.dex	壳列表 / 详细情况 编译器 / dx
classes9.dex	壳列表 / 详细情况 编译器 / dx
