MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

Text Recognize 1.0.0.APK

APP名称:	Text Recognize
包名:	com.tw.identify
域名线索:	18条
URL线索:	26条
邮箱线索:	0条
分析日期:	2022年2月3日 11:20

文件信息

文件名: wzsbk.apk
文件大小: 8.34MB
MD5值: 42292f87950e6ffaa29c2c0e0ff631e7
SHA1值: 85c046e8ff20a50c95c64575b753834a4ab06627
SHA256值: b43d9441e34353413e492f866e0d39016a46c94e2eeaeb369fbdee9ff12b0f8c

APP 信息

App名称: Text Recognize
包名: com.tw.identify
主活动**Activity:** com.tw.identify.ui.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 100

域名线索

域名	是否危险域名	服务器信息
developer.umeng.com	good	**IP:** 59.82.29.163 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
ucc.umeng.com	good	IP: 203.119.169.43 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
plbslog.umeng.com	good	IP: 59.82.66.230 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
xml.apache.org	good	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
ulogs.umengcloud.com	good	IP: 106.11.43.229 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
applog.uc.cn	good	IP: 123.183.235.37 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map
privacy-user-2gtfgjwm96e2ffee-1304234010.tcloudbaseapp.com	good	IP: 121.51.167.29 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
alogus.umeng.com	good	IP: 106.11.86.69 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
ouplog.umeng.com	good	IP: 47.74.172.218 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map

域名	是否危险域名	服务器信息
aip.baidubce.com	good	IP: 111.206.210.12 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
ulogs.umeng.com	good	IP: 106.11.43.142 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
verify.baidubce.com	good	IP: 110.242.69.180 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
gjapplog.ucweb.com	good	IP: 168.235.204.12 所属国家: United States of America 地区: California 城市: Monrovia 纬度: 34.142773 经度: -117.999565 查看地图: Google Map

域名	是否危险域名	服务器信息
api.fanyi.baidu.com	good	IP: 112.80.255.4 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
errlog.umeng.com	good	IP: 106.8.130.60 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810001 经度: 114.879440 查看地图: Google Map
schemas.android.com	good	没有服务器地理信息.
pslog.umeng.com	good	IP: 59.82.29.162 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
alogsus.umeng.com	good	IP: 106.11.43.229 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
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
https://ucc.umeng.com/v1/fetch	com/umeng/analytics/pro/ah.java
https://pslog.umeng.com/ablog	com/umeng/analytics/pro/ah.java
https://aip.baidubce.com/rest/2.0/ocr/v1/bankcard?	com/baidu/ocr/sdk/OCR.java

URL信息	Url所在文件
https://aip.baidubce.com/rest/2.0/ocr/v1/idcard?	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/token/sk?sdkVersion=1_4_4	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1_4_4	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/accurate_basic?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/accurate?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/business_card?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/business_license?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/solution/v1/iocr/recognise?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/driving_license?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general_basic?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general_enhanced?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/general?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/webimage?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/handwriting?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/license_plate?	com/baidu/ocr/sdk/OCR.java

URL信息	Url所在文件
https://aip.baidubce.com/rest/2.0/ocr/v1/lottery?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/numbers?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/passport?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/qrcode?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/receipt?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/vat_invoice?	com/baidu/ocr/sdk/OCR.java
https://aip.baidubce.com/rest/2.0/ocr/v1/vehicle_license?	com/baidu/ocr/sdk/OCR.java
https://verify.baidubce.com/verify/1.0/sdk/report	com/baidu/ocr/sdk/utils/CrashReporterHandler.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://applog.uc.cn/collect	com/uc/crashsdk/a/h.java
https://gjapplog.ucweb.com/collect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
http://schemas.android.com/apk/res-auto	defpackage/ts.java
http://schemas.android.com/apk/res/android	defpackage/p6.java
http://xml.apache.org/xslt}indent-amount	defpackage/bh.java

URL信息	Url所在文件
http://api.fanyi.baidu.com/api/trans/vip/translate	defpackage/ty.java
https://privacy-user-2gtfgjwm96e2ffee-1304234010.tcloudbaseapp.com/privacy.html	Android String Resource
https://privacy-user-2gtfgjwm96e2ffee-1304234010.tcloudbaseapp.com/user.html	Android String Resource
https://applog.uc.cn/collect	lib/armeabi-v7a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://applog.uc.cn/collect	lib/x86/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/x86/libcrashsdk.so
https://errlog.umeng.com	lib/x86/libcrashsdk.so
https://applog.uc.cn/collect	lib/arm64-v8a/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://applog.uc.cn/collect	lib/armeabi/libcrashsdk.so
https://gjapplog.ucweb.com/collect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.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.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.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.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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕
android.permission.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
com.tw.identify.andpermission.bridge	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=china, ST=zhejiang, L=ningbo, O=tsangway.com, OU=tsangway.com, CN=tsangway
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-07-09 04:47:44+00:00
Valid To: 2045-07-03 04:47:44+00:00
Issuer: C=china, ST=zhejiang, L=ningbo, O=tsangway.com, OU=tsangway.com, CN=tsangway
Serial Number: 0x61196275
Hash Algorithm: sha256
md5: 43309004cba77b7dcc51297579ee6aef
sha1: 859ef98c0dd1bf9294d35cbf7bc750a793c06f9e
sha256: bcc88a266015298c9e0af5881f8a200cdb88ea4f215a2f0dcda7a47c58fceb83
sha512: fb75e9c4464ff679c4bbe62e3fa6cf0145957a06fa2baf65bb2a802d9c1b5fd725d7305a74f69b733eb6c07346e99a2c9a12c714271d1e55b763d8a277eb483e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 0ccd6f4d165d5e00949d84420c19743f2075e9db2e726869ab14cfd1f4186fb0

Exodus威胁情报

名称	分类	URL链接
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

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.HARDWARE check
Build.BOARD check
possible Build.SERIAL check
Build.TAGS check
SIM operator check
network operator name check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>lib/arm64-v8a/libumeng-spy.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>emulator file check</td></tr>
</table>
</td></tr>
<tr><td>lib/x86/libumeng-spy.so</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>反虚拟机</td><td>emulator file check</td></tr>
</table>
</td></tr>
</table>
