MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

嘀嗒图片转文字 1.1.5.APK

APP名称:	嘀嗒图片转文字
包名:	com.didiapps.pictoword
域名线索:	31条
URL线索:	35条
邮箱线索:	0条
分析日期:	2022年2月2日 19:30

文件信息

文件名: ddtpzwz518223.apk
文件大小: 3.9MB
MD5值: dfb7c26f642660acfeaa53d811b9a7b2
SHA1值: 5ac289c950601f55f890d1f9bb9efb45ab1de57f
SHA256值: d2b9cc37f6d1b18f81e390f9de3e31f36013929802d698aea839d14354423ddb

APP 信息

App名称: 嘀嗒图片转文字
包名: com.didiapps.pictoword
主活动**Activity:** com.didiapps.pictoword.activity.StartAppActivity
安卓版本名称: 1.1.5
安卓版本: 10

域名线索

域名	是否危险域名	服务器信息
mta.oa.com	good	**IP:** 193.123.33.15 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam 纬度: 52.374031 经度: 4.889690 查看地图: Google Map

域名	是否危险域名	服务器信息
aaid.umeng.com	good	IP: 106.8.130.61 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
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
paypictoword.dida110.com	good	IP: 121.43.198.112 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
mclient.alipay.com	good	IP: 203.209.250.50 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
plbslog.umeng.com	good	IP: 106.11.223.204 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
xihu.chexr.cc	good	IP: 121.43.198.112 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
ulogs.umeng.com	good	IP: 106.11.86.77 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
mcgw.alipay.com	good	IP: 203.209.250.50 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
alogsus.umeng.com	good	IP: 59.82.29.246 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
developer.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
errlog.umeng.com	good	IP: 116.132.223.36 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
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
pingma.qq.com	good	IP: 119.45.78.184 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
mobilegw.stable.alipay.net	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
pslog.umeng.com	good	IP: 59.82.31.160 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
schemas.android.com	good	没有服务器地理信息.
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	IP: 110.75.132.131 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.mch.weixin.qq.com	good	IP: 182.254.22.146 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
mobilegw.alipay.com	good	IP: 203.209.245.77 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: 47.74.172.6 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
m.alipay.com	good	IP: 203.209.245.120 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
alogus.umeng.com	good	IP: 59.82.29.246 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
mta.qq.com	good	IP: 220.194.87.235 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
ulogs.umengcloud.com	good	IP: 203.119.174.133 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
wappaygw.alipay.com	good	IP: 203.209.250.6 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
errlogos.umeng.com	good	IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map

域名	是否危险域名	服务器信息
loggw-exsdk.alipay.com	good	IP: 203.209.238.2 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: 112.80.255.237 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
h5.m.taobao.com	good	IP: 140.249.89.233 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java

URL信息	Url所在文件
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/app/PayTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java

URL信息	Url所在文件
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
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/i.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
http://mta.qq.com/	com/tencent/wxop/stat/z.java

URL信息	Url所在文件
http://mta.oa.com/	com/tencent/wxop/stat/z.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/x.java
https://aip.baidubce.com/rest/2.0/ocr/v1/bankcard?	com/baidu/ocr/sdk/OCR.java
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

URL信息	Url所在文件
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
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://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java

URL信息	Url所在文件
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://api.mch.weixin.qq.com/pay/unifiedorder	com/didiapps/pictoword/c/b/c.java
http://paypictoword.dida110.com/notify_url_wx.aspx	com/didiapps/pictoword/c/b/c.java
http://paypictoword.dida110.com/notify_url.aspx	com/didiapps/pictoword/c/a/a.java
http://xihu.chexr.cc/rule_yh.html	com/didiapps/pictoword/activity/AboutActivity.java
http://xihu.chexr.cc/rule_yh.html	com/didiapps/pictoword/activity/MoreActivity.java
http://xihu.chexr.cc/rule_ys.html	com/didiapps/pictoword/activity/MoreActivity.java
http://xihu.chexr.cc/rule_ys.html	com/didiapps/pictoword/activity/StartAppActivity.java
http://xihu.chexr.cc/rule_yh.html	com/didiapps/pictoword/activity/StartAppActivity.java
http://xihu.chexr.cc/	com/didiapps/pictoword/d/k.java
http://schemas.android.com/apk/res/android	b/c/a/f.java
https://h5.m.taobao.com/mlapp/olist.html	b/a/b/b/a.java
https://mcgw.alipay.com/sdklog.do	b/a/b/f/f/c.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	b/a/b/f/f/d.java

URL信息	Url所在文件
https://mobilegw.alipay.com/mgw.htm	b/a/b/a/a.java
https://mobilegw.alipaydev.com/mgw.htm	b/a/b/j/k.java
http://m.alipay.com/?action=h5quit	b/a/b/j/l.java
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/x86/libcrashsdk.so
https://errlog.umeng.com	lib/x86/libcrashsdk.so
https://errlogos.umeng.com	lib/x86/libcrashsdk.so
https://errlog.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/arm64-v8a/libcrashsdk.so
https://errlog.umeng.com	lib/arm64-v8a/libcrashsdk.so
https://errlogos.umeng.com	lib/arm64-v8a/libcrashsdk.so

URL信息	Url所在文件
https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi/libcrashsdk.so
https://errlogos.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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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

向手机申请的权限	是否危险	类型	详细情况
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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=cn, ST=zj, L=hz, O=dd, OU=dd, CN=com.didiapps.pictoword
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-08-27 08:32:01+00:00
Valid To: 2567-03-27 08:32:01+00:00
Issuer: C=cn, ST=zj, L=hz, O=dd, OU=dd, CN=com.didiapps.pictoword
Serial Number: 0x18340ea3
Hash Algorithm: sha256
md5: 443c9d81afa443697b128774284075ac
sha1: 0dde9a11ceba17ca685f630f3e429d586882f7c8
sha256: 800b41d1b3fe254c939128295ac720d1c823af2c88374d43d5601478d4bc1e44
sha512: a01336fd7430d90da61fafe930f47b7575421063ac56e484cecd4b0a7886bfc086c26f35ab5af02fbb00dda5463dbc2cac4b0330ff1257ae28a2cd6ad5006998
PublicKey Algorithm: rsa
Bit Size: 2048

Fingerprint: 0fdb04f8f9829c471a007e71ef4fe65b3a614b90bf1b2f2890025facd2f81208

Exodus威胁情报

名称	分类	URL链接
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	<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 device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>

文件列表	分析结果
