MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

掌上云勤 1.0.0.APK

APP名称:	掌上云勤
包名:	com.fskj.attendance
域名线索:	41条
URL线索:	39条
邮箱线索:	1条
分析日期:	2022年2月3日 13:43

文件信息

文件名: zsyq.apk
文件大小: 7.83MB
MD5值: 9f830cf1c20f541f78457e65f2002aca
SHA1值: e9fc156cdc67d93256dbf9c050c0ed1c22fbc922
SHA256值: 0293cd60e4ca812efd2a94cb5ff3accf0ab183fd4ced69232eebc828f885818f

APP 信息

App名称: 掌上云勤
包名: com.fskj.attendance
主活动**Activity:** com.fskj.attendance.login.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
www.ntsc.ac.cn	good	**IP:** 117.23.61.159 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.560280 查看地图: Google Map

域名	是否危险域名	服务器信息
open.weixin.qq.com	good	**IP:** 109.244.144.48 **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
www.51miaomiao.compf	good	没有服务器地理信息.
dualstack.apilocate.amap.com	good	**IP:** 106.11.40.50 **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
www.wireless-village.org	good	**IP:** 172.67.131.214 **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
mobilegw.aaa.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
yule-app-public-prod.oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.219 **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
render.alipay.com	good	**IP:** 150.138.144.196 **所属国家:** China **地区:** Shandong **城市:** Qingdao **纬度:** 36.098610 **经度:** 120.371941 **查看地图:** Google Map
restsdk.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
h5.m.taobao.com	good	**IP:** 60.28.226.42 **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

域名	是否危险域名	服务器信息
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
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
schemas.xmlsoap.org	good	**IP:** 104.102.119.246 **所属国家:** United States of America **地区:** Massachusetts **城市:** Billerica **纬度:** 42.558430 **经度:** -71.268951 **查看地图:** Google Map
web.ifishfun.com	good	**IP:** 47.111.243.178 **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
www.51miaomiao.commldip1992180694mldipi1887204221uartinfo0	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
lbs.amap.com	good	**IP:** 59.82.29.231 **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
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
long.open.weixin.qq.com	good	**IP:** 109.244.217.35 **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
mclient.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

域名	是否危险域名	服务器信息
dualstack-restsdk.amap.com	good	**IP:** 39.98.22.142 **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
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
xmlpull.org	good	**IP:** 74.50.61.58 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.814899 **经度:** -96.879204 **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
www.51miaomiao.com	good	**IP:** 118.190.67.214 **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
mcgw.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
abroad.apilocate.amap.com	good	**IP:** 59.82.34.246 **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
mobilegw.alipay.com	good	**IP:** 203.209.255.238 **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
www.buz.org	good	**IP:** 208.113.162.199 **所属国家:** United States of America **地区:** California **城市:** Brea **纬度:** 33.930222 **经度:** -117.888420 **查看地图:** Google Map

域名	是否危险域名	服务器信息
yule-app-name.oss-cn-hangzhou.aliyuncs.com	good	**IP:** 118.31.219.219 **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:** 59.82.60.56 **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
192.168.10.83	good	**IP:** 192.168.10.83 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
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

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
webdev.fangsheng.tech	good	**IP:** 47.98.219.38 **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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
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

域名	是否危险域名	服务器信息
www.openmobilealliance.org	good	**IP:** 104.26.9.105 **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
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
loggw-exsdk.alipay.com	good	**IP:** 110.75.134.9 **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
www.w3.org	good	**IP:** 128.30.52.100 **所属国家:** United States of America **地区:** Massachusetts **城市:** Cambridge **纬度:** 42.365078 **经度:** -71.104523 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.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/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java

URL信息	Url所在文件
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://web.ifishfun.com/	com/fskj/applibrary/base/Constant.java
https://webdev.fangsheng.tech/	com/fskj/applibrary/base/Constant.java
https://yule-app-public-prod.oss-cn-hangzhou.aliyuncs.com/	com/fskj/applibrary/base/Constant.java
https://yule-app-name.oss-cn-hangzhou.aliyuncs.com/	com/fskj/applibrary/base/Constant.java
https://)?((?:	com/fskj/applibrary/util/NetWorkUtil.java
http://www.ntsc.ac.cn/	com/fskj/applibrary/util/NetTimeUtil.java
http://www.buz.org/buzService/	com/cncrit/qiaoqiao/WebService.java
http://192.168.10.83:91/axis2/services/buzService?wsdl	com/cncrit/qiaoqiao/WebService.java

URL信息	Url所在文件
http://abroad.apilocate.amap.com/mobile/binary	com/loc/en.java
http://restsdk.amap.com	com/loc/s.java
http://apilocate.amap.com/mobile/binary	com/loc/ej.java
http://dualstack.apilocate.amap.com/mobile/binary	com/loc/ej.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ej.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ec.java
http://dualstack-restsdk.amap.com/v3/geocode/regeo	com/loc/ee.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/ee.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cb.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/l.java
http://restsdk.amap.com/v3/iasdkauth	com/loc/l.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/f.java

URL信息	Url所在文件
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
http://mta.qq.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://mta.oa.com/	com/tencent/wxop/stat/StatServiceImpl.java
http://pingma.qq.com:80/mstat/report	com/tencent/wxop/stat/common/StatConstants.java
www.51miaomiao.com&MlDip=1992180694&MlDipI=1887204221&UartInfo=0	com/miot/android/sdk/MiotLink_4004_Info.java
www.51miaomiao.com&pf_port=28001&pf_ip1=118.190.67.214&pf_ip2=122.225.196.132&	com/miot/android/sdk/MiotLink_4004_Info.java
www.51miaomiao.com	com/miot/android/sdk/MiotLink_4004_Info.java
http://www.buz.org/buzService/	com/miot/android/content/NoFormatConsts.java
www.51miaomiao.com	com/miot/android/content/NoFormatConsts.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
http://xmlpull.org/v1/doc/properties.html#xmldecl-standalone	org/kxml2/kdom/Document.java
http://www.w3.org/XML/1998/namespace	org/kxml2/wap/WbxmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/wap/WbxmlParser.java
http://www.	org/kxml2/wap/wml/Wml.java
https://www.	org/kxml2/wap/wml/Wml.java

URL信息	Url所在文件
http://www.wireless-village.org/CSP	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/PA	org/kxml2/wap/wv/WV.java
http://www.wireless-village.org/TRC	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-CSP	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-PA	org/kxml2/wap/wv/WV.java
http://www.openmobilealliance.org/DTD/WV-TRC	org/kxml2/wap/wv/WV.java
www.wireless-village.org	org/kxml2/wap/wv/WV.java
http://xmlpull.org/v1/doc/features.html#indent-output	org/kxml2/io/KXmlSerializer.java
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlSerializer.java
http://xmlpull.org/v1/doc/	org/kxml2/io/KXmlParser.java
http://www.w3.org/XML/1998/namespace	org/kxml2/io/KXmlParser.java
http://www.w3.org/2000/xmlns/	org/kxml2/io/KXmlParser.java
http://schemas.xmlsoap.org/soap/encoding/	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2003/05/soap-encoding	org/ksoap2/SoapEnvelope.java
http://schemas.xmlsoap.org/soap/envelope/	org/ksoap2/SoapEnvelope.java

URL信息	Url所在文件
http://www.w3.org/2003/05/soap-envelope	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema	org/ksoap2/SoapEnvelope.java
http://www.w3.org/2001/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://www.w3.org/1999/XMLSchema-instance	org/ksoap2/SoapEnvelope.java
http://xml.apache.org/xml-soap	org/ksoap2/serialization/MarshalHashtable.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes	org/xmlpull/v1/XmlPullParser.java
http://xmlpull.org/v1/doc/features.html#validation	org/xmlpull/v1/XmlPullParser.java
https://github.com/vinc3m1	Android String Resource
https://github.com/vinc3m1/RoundedImageView	Android String Resource
https://github.com/vinc3m1/RoundedImageView.git	Android String Resource

邮箱线索

邮箱地址	所在文件
3122469463@qq.com	com/fskj/attendance/mine/ServiceActivity.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.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_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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: ST=zhejiang, L=hangzhou, O=zhijia, CN=zhijia
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-09-13 02:54:54+00:00
Valid To: 2046-09-07 02:54:54+00:00
Issuer: ST=zhejiang, L=hangzhou, O=zhijia, CN=zhijia
Serial Number: 0x7731a4cc
Hash Algorithm: sha256

md5: 98ca58e0e3303f32023e978ac8e3a243
sha1: ee1f449ebe24825d6568a21420c7d13eded8f03c
sha256: e6a6bc4e349d7442eda5d07afdff09efff391c183bd332626b99714c61e00a92
sha512: 6a44bb3ee2f5d0cd674f9ff931577a50b629ffff066850dc47da35edb2a7e7492d2ce553dd9796d30ffcd8c8477957ee89758f18a9c72f4ff3c14c0a484a7494
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: bfa4e083060bfbe4463d098146b0cdfceb6192279e6d3f271bb2591cf660c002

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Tencent Stats	Analytics	https://reports.exodus-privacy.eu.org/trackers/116

硬编码敏感信息

可能的敏感信息
"library_roundedimageview_author" : "Vince Mi"
"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

加壳分析

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 without marker (suspicious)</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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
subscriber ID check</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
