MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

咚咚燕助手 1.4.0.APK

APP名称:	咚咚燕助手
包名:	com.wdcloud.jiafuassistant
域名线索:	9条
URL线索:	31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: ddyzs.apk
文件大小: 8.4MB
MD5值: 45bdadcaf07419711e1a786d76e83a68
SHA1值: 575219f9dce34a3bbfd682d1486708c9a3f355b7
SHA256值: cc043e70b88dd7fb3ab40a5175b92ab2aed5b59f95b870e3c8bd785cd63bd53d

APP 信息

App名称: 咚咚燕助手
包名: com.wdcloud.jiafuassistant
主活动**Activity:** com.wdcloud.pandaassistant.module.splash.activity.SplashActivity
安卓版本名称: 1.4.0
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
hrss-api.wdeduc.com	good	**IP:** 123.57.153.43 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
hrss-main.wdeduc.com	good	**IP:** 123.57.153.43 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
homemaking.wdeduc.com	good	**IP:** 182.40.19.221 **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
long.open.weixin.qq.com	good	**IP:** 109.244.216.15 **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
sdjz-h5.dongdongjz.com	good	**IP:** 42.81.213.231 **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
open.weixin.qq.com	good	**IP:** 175.24.219.72 **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
ns.adobe.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
ddyx.wdeduc.com	good	**IP:** 123.57.153.43 **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
schemas.android.com	good	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://homemaking.wdeduc.com/remind/list?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/auntieList?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/resume?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/re-mall?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://sdjz-h5.dongdongjz.com/insurance?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/applyGoods/list?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/earnings-manage	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java

URL信息	Url所在文件
https://homemaking.wdeduc.com/business?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://homemaking.wdeduc.com/message?statusBarHeight=	com/wdcloud/pandaassistant/module/home/view/HomeFragment.java
https://ddyx.wdeduc.com/	com/wdcloud/pandaassistant/module/doorpass/search/SearchApplyDoorPassListActivity.java
https://ddyx.wdeduc.com/	com/wdcloud/pandaassistant/module/doorpass/list/ApplyDoorPassListActivity.java
https://homemaking.wdeduc.com/schedule	com/wdcloud/pandaassistant/module/contract/scheduletable/view/ScheduleH5TableActivity.java
https://sdjz-h5.dongdongjz.com/	com/wdcloud/pandaassistant/module/contract/explain/view/ContractPayWebActivity.java
https://sdjz-h5.dongdongjz.com/contractPay?isWeiXin=	com/wdcloud/pandaassistant/module/contract/explain/view/ContractPayWebActivity.java
https://homemaking.wdeduc.com/contractEdit?uuid=	com/wdcloud/pandaassistant/module/contract/checkpdf/CheckContractDetailActivity.java
https://homemaking.wdeduc.com/contractReview?type=1&id=	com/wdcloud/pandaassistant/module/contract/template/ContractPreviewActivity.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://ns.adobe.com/xap/1.0/	b/n/a/a.java

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	b/j/b/c/g.java
https://homemaking.wdeduc.com/	e/i/a/b/t/b/e.java
https://hrss-main.wdeduc.com/	e/i/a/c/a/b.java
https://hrss-api.wdeduc.com/	e/i/a/c/a/b.java
https://hrss-api.wdeduc.com/gx-homemaking/v1/common/uploadImages	e/i/a/c/a/b.java
https://hrss-api.wdeduc.com/operate/v1/version/getInfo	e/i/a/d/g.java
http://schemas.android.com/apk/res-auto	e/g/a/a/i/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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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

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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.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.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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=000000, ST=bj, L=bj, O=org, OU=org, CN=weidong
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-25 03:17:23+00:00
Valid To: 2046-06-19 03:17:23+00:00
Issuer: C=000000, ST=bj, L=bj, O=org, OU=org, CN=weidong
Serial Number: 0x797c666d
Hash Algorithm: sha256
md5: 471adee67ec08bc44a58b8d9739b3206
sha1: 52893846cb18a426c4e537627d68c89e50defae6
sha256: 45a6c37fc04b0d620cd00e355775560701d366f55f2b0d2be8c5b42c5706dc07
sha512: b96caa5bd264e6fa15e44a56d011e20ba2f08131aee85e6642aebe014326f2b102d2ef7c8284064d3221e79a21dcdf8abfab09d660e73cb91a477690fa61c7f4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 35602c76964fbc7f5c78ff9d84fa1c6a37e2ac74a459109937131562b95f0d6e

硬编码敏感信息

可能的敏感信息
"find_password" : "找回密码"
"forget_password" : "忘记密码?"
"input_login_pwd" : "密码默认手机后4位(数字或字母)"
"legal_person_authorization" : "企业法人授权"
"login_pwd" : "登录密码"

可能的敏感信息
"password" : "密码"
"tv_login_type_pwd" : "密码登录"
"tv_pwd_again_tip" : "请再次输入密码"
"tv_pwd_length_desc" : "密码必须为6–20位数字加字母组合"
"tv_pwd_length_not_same" : "两次输入不一致，请重新输入"
"tv_pwd_tip" : "请输入密码（区分大小写）"
"tv_reset_password" : "重置密码"
"tv_reset_pwd_tips" : "管理员修改了密码强度 你的密码过于简单, 建议您修改密码"
"tv_set_password" : "设置密码"

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.FINGERPRINT check
Build.MANUFACTURER check</td></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
<tr><td>classes2.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
