Evaluation Warning: The document was created with Spire.Doc for Python.

**91858.com（ 1.2.1版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 91858.com |
| 版本 | 1.2.1 |
| 包名 | com.mv1209xzf.dvlx |
| 域名线索 | 30条 |
| URL线索 | 25条 |
| APP图标 |  |
| 分析日期 | 2025年6月12日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 105974989.apk |
| 文件大小 | 71.25MB |
| MD5值 | 4e391727223d07e1f903012e1803437e |
| SHA1值 | 575d66567471e0b55b657d3425be03212e98dbee |
| SHA256值 | 3998d3e61e43df0a7f3fa1f25110e137136536eb30107e915a05c86629ab6ceb |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 91858.com |
| 包名 | com.mv1209xzf.dvlx |
| 主活动Activity | com.mv1209xzf.dvlx.MainActivity |
| 安卓版本名称 | 1.2.1 |
| 安卓版本 | 1210 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| api.uca.cloud.unity3d.com | IP: 43.156.88.56 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 182.92.20.189 | IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing  |
| www.taobao.com | IP: 125.39.135.39 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| mta.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| code.google.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| bjuser.jpush.cn | IP: 122.9.15.248 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| esotericsoftware.com | IP: 139.162.66.173 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| img.alicdn.com | IP: 123.6.7.213 所属国家: China 地区: Henan 城市: Zhengzhou  |
| open.weixin.qq.com | IP: 140.207.58.67 所属国家: China 地区: Shanghai 城市: Shanghai  |
| static.youku.com | IP: 42.59.4.117 所属国家: China 地区: Liaoning 城市: Dalian  |
| cloudaemon.com | IP: 203.107.45.167 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| config.uca.cloud.unity3d.com | IP: 34.111.113.40 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.openssl.org | IP: 184.50.93.94 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api.weixin.qq.com | IP: 112.65.193.153 所属国家: China 地区: Shanghai 城市: Shanghai  |
| tsis.jpush.cn | IP: 120.46.73.159 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| daup.map.baidu.com | IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding  |
| mail.qq.com | IP: 157.148.58.29 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| cdp.cloud.unity3d.com | IP: 43.156.88.56 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| pingma.qq.com | IP: 116.147.19.64 所属国家: China 地区: Beijing 城市: Beijing  |
| loc.map.baidu.com | IP: 111.206.209.175 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.209.166 所属国家: China 地区: Beijing 城市: Beijing  |
| sina.cn | IP: 123.125.107.21 所属国家: China 地区: Beijing 城市: Beijing  |
| ofloc.map.baidu.com | IP: 110.242.70.118 所属国家: China 地区: Hebei 城市: Baoding  |
| 1212.ip138.com | IP: 110.81.155.137 所属国家: China 地区: Fujian 城市: Quanzhou  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| mta.oa.com | IP: 141.144.196.217 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| www.jd.com | IP: 119.188.208.2 所属国家: China 地区: Shandong 城市: Zaozhuang  |
| long.open.weixin.qq.com | IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://bjuser.jpush.cn/v1/appawake/status  | cn/jiguang/aa/b.java  |
| https://tsis.jpush.cn  | cn/jiguang/ad/i.java  |
| http://182.92.20.189:9099/  | cn/jiguang/o/c.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/a/f.java  |
| http://loc.map.baidu.com/cc.php  | com/baidu/location/a/d.java  |
| http://loc.map.baidu.com/gpsz  | com/baidu/location/b/a.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/d/g.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/d/k.java  |
| http://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/d/h.java  |
| http://%s/%s  | com/baidu/location/d/d.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/d/d.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/tcu.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/g/j.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/g/j.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/g/j.java  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | com/baidu/location/indoor/a.java  |
| http://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/indoor/mapversion/b/a.java  |
| http://1212.ip138.com/ic.asp  | com/cloudaemon/libguandujni/GuanduJNI.java  |
| https://api.weixin.qq.com/sns/userinfo?access\_token=  | com/mv1209xzf/dvlx/MainActivity.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid=  | com/mv1209xzf/dvlx/MainActivity.java  |
| https://api.weixin.qq.com/sns/auth?access\_token=  | com/mv1209xzf/dvlx/MainActivity.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?appid=  | com/mv1209xzf/dvlx/MainActivity.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/d.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.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  |
| http://code.google.com/p/protobuf-net/  | lib/armeabi-v7a/libil2cpp.so  |
| http://esotericsoftware.com/spine-unity-documentation  | lib/armeabi-v7a/libil2cpp.so  |
| https://github.com/pharan/spine-unity-docs/blob/master/SkeletonRenderSeparator.md  | lib/armeabi-v7a/libil2cpp.so  |
| https://api.uca.cloud.unity3d.com/v1/events  | lib/armeabi-v7a/libunity.so  |
| https://cdp.cloud.unity3d.com/v1/events  | lib/armeabi-v7a/libunity.so  |
| https://config.uca.cloud.unity3d.com  | lib/armeabi-v7a/libunity.so  |
| http://mail.qq.com/  | lib/armeabi-v7a/libyunceng.so  |
| http://static.youku.com/ddshow/img/static/js/jquery.js  | lib/armeabi-v7a/libyunceng.so  |
| http://sina.cn  | lib/armeabi-v7a/libyunceng.so  |
| http://img.alicdn.com/tps1/i1/T1FeW3XXNfXXXXXXXX-36-36.gif  | lib/armeabi-v7a/libyunceng.so  |
| http://www.baidu.com  | lib/armeabi-v7a/libguandu.so  |
| https://www.jd.com  | lib/armeabi-v7a/libguandu.so  |
| https://www.taobao.com  | lib/armeabi-v7a/libguandu.so  |
| http://cloudaemon.com/howto.html  | lib/armeabi-v7a/libguandu.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libguandu.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sales@openvpn.net  | lib/armeabi-v7a/libguandu.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**无法读取代码签名证书.**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "PASSWORD" : "Password"  |
| "USERNAME" : "Username"  |
| "PASSWORD" : "Adgangskode"  |
| "USERNAME" : "Brugernavn"  |
| "PASSWORD" : "パスワード"  |
| "USERNAME" : "ユーザー名"  |
| "PASSWORD" : "Passwort"  |
| "USERNAME" : "Nutzername"  |
| "PASSWORD" : "密码"  |
| "USERNAME" : "用户名"  |
| "PASSWORD" : "Mật khẩu"  |
| "USERNAME" : "Tên đăng nhập"  |
| "PASSWORD" : "Wachtwoord"  |
| "USERNAME" : "Gebruikersnaam"  |
| "PASSWORD" : "암호"  |
| "USERNAME" : "사용자 이름"  |
| "PASSWORD" : "Mot de passe"  |
| "USERNAME" : "Nom d'utilisateur"  |
| "PASSWORD" : "Contraseña"  |
| "USERNAME" : "Nombre de usuario"  |
| "PASSWORD" : "Parola d'ordine"  |
| "USERNAME" : "Nome utente"  |
| "PASSWORD" : "Senha"  |
| "USERNAME" : "Nome de usuário"  |
| "PASSWORD" : "пароль"  |
| "USERNAME" : "имя пользователя"  |
| "PASSWORD" : "Lösenord"  |
| "USERNAME" : "Användarnamn"  |
| "PASSWORD" : "密碼"  |
| "USERNAME" : "用戶名"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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 |
| --- | --- | --- | --- |
| com.mv1209xzf.dvlx.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| 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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_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.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.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.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.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.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.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.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.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.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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.MANAGE\_DOCUMENTS | 合法 |  | 允许应用程序管理对文档的访问,通常作为文档选择器的一部分 |
| android.hardware.camera.autofocus | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.mv1209xzf.dvlx.MainActivity | **Schemes**: com.mv1209xzf.dvlx://, **Hosts:** data, **Path Prefixes:** /openwith,  |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**