



DST 124.APK 分析报告



APP名称:

DST

包名:	uni.UNI1ED8AEB
域名线索:	34条
URL线索:	28条
邮箱线索:	3条
分析日期:	2024年4月24日
分析平台:	摸瓜反编译平台

文件名: uni.UNI1ED8AEB.apk
文件大小: 55.56MB
MD5值: 3d3419e6cd372ca77001da62b03ada3c
SHA1值: 9307b3b9c1bf9ad0df66be4a7058c0aa39afc006
SHA256值: 2e073846a16e175f318794f9312e60ffb01cf33f4981dc7553bd709b250210ec

i APP 信息

App名称: DST
包名: uni.UNI1ED8AEB
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 124
安卓版本: 124

🔍 域名线索

域名	服务器信息
cdn.uviewui.com	IP: 150.138.98.116 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
www.google.com	IP: 199.96.59.95 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
8.134.52.225	IP: 8.134.52.225 所属国家: China 地区: Zhejiang

	城市: Hangzhou 纬度: 30.293650 经度: 120.161423
quilljs.com	IP: 216.24.57.3 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
stjjblog.oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.225 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
apiba.dst88.vip	没有服务器地理信息.
www.dst88.vip	IP: 47.243.74.130 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.w3.org	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
momentjs.com	IP: 104.16.153.25 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

crbug.com	IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.openssl.org	IP: 23.13.92.35 所属国家: Malaysia 地区: Selangor 城市: Cyberjaya 纬度: 2.922500 经度: 101.654999
apiaa.dst88.vip	没有服务器地理信息.
ask.dcloud.net.cn	IP: 122.228.95.183 所属国家: China 地区: Zhejiang 城市: Wenzhou 纬度: 27.999420 经度: 120.666817
im.amoa.cn	IP: 125.88.215.135 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
github.com	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
	IP: 45.113.202.151

45.113.202.151	所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435829
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571
schemas.android.com	没有服务器地理信息.
apiab.dst88.vip	没有服务器地理信息.
at.alicdn.com	IP: 106.119.193.228 所属国家: China 地区: Hebei 城市: Tangshan 纬度: 39.633331 经度: 118.183327
apis.map.qq.com	IP: 109.244.244.109 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
m3w.cn	IP: 122.228.74.145 所属国家: China 地区: Zhejiang 城市: Wenzhou 纬度: 27.999420 经度: 120.666817
	IP: 8.134.118.40

8.134.118.40	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
apiad.dst88.vip	没有服务器地理信息.
up.myap.vip	没有服务器地理信息.
apiac.dst88.vip	没有服务器地理信息.
lame.sf.net	IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047
stream.mobihTML5.com	IP: 112.80.255.152 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777779
registry.npmjs.org	IP: 104.16.19.35 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
stream.dcloud.net.cn	IP: 118.31.71.109 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

ns.adobe.com	没有服务器地理信息.
service.dcloud.net.cn	IP: 47.97.121.192 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
103.8.222.71	IP: 103.8.222.71 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435829
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	IP: 47.93.95.208 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

 URL线索

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/283	io/dcloud/h/b.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java

https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/c/h/b.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/f/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/b/a.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobihhtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	Mogua Engine V2
https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2

http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://github.com/crypto-browserify/crypto-browserify	Mogua Engine V2
https://up.myap.vip/api/index/universion	Mogua Engine V2
https://registry.npmjs.org/elliptic/-/elliptic-6.5.2.tgz	Mogua Engine V2
https://github.com/indutny/elliptic/issues	Mogua Engine V2
https://github.com/indutny/elliptic	Mogua Engine V2
https://github.com/emn178/js-md5	Mogua Engine V2
http://im.amoa.cn:213	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
">http://www.w3.org/2000/svg'>	Mogua Engine V2
https://cdn.uviewui.com/uview/resources/video.mp4	Mogua Engine V2
https://cdn.uviewui.com/uview/swiper/swiper1.png	Mogua Engine V2
https://cdn.uviewui.com/uview/swiper/swiper3.png	Mogua Engine V2
https://cdn.uviewui.com/uview/swiper/swiper2.png	Mogua Engine V2
http://stjjblog.oss-cn-hangzhou.aliyuncs.com/10d92cae0adc0d7ac0564d65dd528266.webp	Mogua Engine V2

http://feross.org >	Mogua Engine V2
https://8.134.118.40	Mogua Engine V2
http://8.134.52.225:99	Mogua Engine V2
http://45.113.202.151:88	Mogua Engine V2
https://apiba.dst88.vip	Mogua Engine V2
http://momentjs.com/guides/	Mogua Engine V2
https://apiaa.dst88.vip	Mogua Engine V2
https://apiab.dst88.vip	Mogua Engine V2
https://apiac.dst88.vip	Mogua Engine V2
https://apiad.dst88.vip	Mogua Engine V2
https://www.dst88.vip	Mogua Engine V2
http://103.8.222.71:88	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2
https://quilljs.com	Mogua Engine V2
https://crbug.com/v8/8520	lib/x86/libweexjss.so
http://lame.sf.net	lib/x86/liblamemp3.so
http://www.openssl.org/support/faq.html	lib/x86/libijkffmpeg.so

https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so
http://lame.sf.net	lib/arm64-v8a/liblamemp3.so

 邮箱线索

邮箱地址	所在文件
fedor@indutny.com git@github.com emn178@gmail.com abc@yoo.com jhruby.web@gmail.com tgtags@2x.png	Mogua Engine V2
icon-ipad-app@2x.png on-ipad-notification@2x.png icon-ipad-proapp@2x.png icon-ipad-settings@2x.png icon-ipad-spotlight@2x.png icon-iphone-app@2x.png icon-iphone-app@3x.png -iphone-notification@2x.png -iphone-notification@3x.png icon-iphone-settings@2x.png icon-iphone-settings@3x.png con-iphone-spotlight@2x.png con-iphone-spotlight@3x.png	Mogua Engine V2
ffmpeg-devel@ffmpeg.org	lib/x86/libijkplayer.so

 手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java
19919152923	Mogua Engine V2
18651669817	Mogua Engine V2

🌟 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=cn, ST=shanghai, L=shanghai, O=恒上商务, OU=恒上商务, CN=恒上商务
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-06-22 13:03:21+00:00
Valid To: 2046-06-16 13:03:21+00:00
Issuer: C=cn, ST=shanghai, L=shanghai, O=恒上商务, OU=恒上商务, CN=恒上商务
Serial Number: 0x500f8ab
Hash Algorithm: sha256
md5: 8c649bcb2c2fcb284fe1f392a4cc1fe2
sha1: 521023cde3b616241d32f78ec7b52122dc87c72c
sha256: a11b1562f4563f8fd3ad58fb76137ab05e05f604912d3e752c25670b0c1719e1
sha512: 9ecf3cf026544317c6088005607e1c7a29816793cce32649c8ad746712b3e61ec5202bac7118f4dcc1cc1794fd9658448a884c981aad0fd2fc4c1f3fb219dac7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: e233ed095e167b22134bbab67fd858b7c97b562ad56d650b3bdd1ab6431882e3

🔑 硬编码敏感信息

可能的敏感信息

"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"
"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"

 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.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.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
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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_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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference

应用内通信