



MoGua

霍英东集团 1.0.9.APK 分析报告



APP名称:

霍英东集团

包名:	uni.app.UNI2C0111F
域名线索:	15条
URL线索:	23条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件名: 霍英东[1].apk
文件大小: 73.73MB
MD5值: 4f3c3d0da93df8ebd2e84aca171edac7
SHA1值: 0e07eff70aaedbd1af150af8569fbc63dfefe818
SHA256值: b584b1fc4a8c4f6f3a49268591a37753f276fd65ea53c46d9f6d12fed69becd5

i APP 信息

App名称: 霍英东集团
包名: uni.app.UNI2C0111F
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.9
安卓版本: 109

🔍 域名线索

域名	服务器信息
mdc.html5.qq.com	IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
m3w.cn	IP: 221.204.20.165 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
log.tbs.qq.com	IP: 124.95.231.218 所属国家: China 地区: Liaoning

	城市: Shenyang 纬度: 41.792221 经度: 123.432877
er.dcloud.io	没有服务器地理信息.
tbs.imtt.qq.com	IP: 211.93.212.232 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ask.dcloud.net.cn	IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tbsrecovery.imtt.qq.com	IP: 60.28.172.40 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
pms.mb.qq.com	IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
schemas.android.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000

	经度: 0.000000
debugtbs.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
ns.adobe.com	没有服务器地理信息.
cfg.imtt.qq.com	IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
debugx5.qq.com	IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
mqqad.html5.qq.com	IP: 0.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047&is64=0	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047&is64=1	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041&is64=0	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041&is64=1	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java

https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utls/o.java
https://mqqqad.html5.qq.com/adjs	com/tencent/smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utls/o.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utls/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utls/d.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java

https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.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
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

邮箱线索

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=CN, ST=Shanghai, L=Shanghai, O=Hyd Company, OU=Hyd Team, CN=Hydrogen
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-10 01:45:23+00:00
有效期至: 2052-10-26 01:45:23+00:00
发行人: C=CN, ST=Shanghai, L=Shanghai, O=Hyd Company, OU=Hyd Team, CN=Hydrogen
序列号: 0xb965d5a8166e7e42
哈希算法: sha256
md5值: efe372a69c000a5945b1aeb663b434db

sha1值: e88710ccd3f54b0c37e03902a7665db03c701e80

sha256值: d5f7646e36d02aa597eaabf45f86209decd443d72219c132308c9fc6474fd09b

sha512值: ee28536ede842555a7c118b7aa0f2a79e8e71e9b18a2a253b3272cc1cf7172791695e800324936e2da4fcdabd7b77e418af59948e5800e6b24e1ea29194471d5

公钥算法: rsa

密钥长度: 2048

指纹: 912e46935814b894f62f8c53baf104e3d2997f879a8518ebadd8f23c7ffb0fc

 硬编码敏感信息

 加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

 第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

 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.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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

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