MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

振鑫隆域
ZHEN XIN LONG YU

振鑫隆域 1.0.0.APK

APP名称:	振鑫隆域
包名:	zhenxinlongyuanzhuo.lxkj8.com
域名线索:	7条
URL线索:	37条
邮箱线索:	0条
分析日期:	2022年1月25日 23:06

文件信息

文件名: zhenxinlongyu578245.apk
文件大小: 4.38MB
MD5值: 9b94a3d94e2d6e073ef1a90af4b49511
SHA1值: 4fe3683d25d341224428086f62d7148c10984bf2
SHA256值: ff787d0ec56d9acf22d9aedba92d51ef60e7ca73af15b7ad41715a3e27a87b04

APP 信息

App名称: 振鑫隆域
包名: zhenxinlongyuanzhuo.lxkj8.com
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0.0
安卓版本: 2

域名线索

域名	是否危险域名	服务器信息
schemas.android.com	good	没有服务器地理信息.
96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com	good	**IP:** 47.93.95.208 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
stream.dcloud.net.cn	good	**IP:** 118.31.188.88 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
m3w.cn	good	**IP:** 125.37.206.223 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
ask.dcloud.net.cn	good	**IP:** 124.239.227.208 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717 查看地图: Google Map
stream.mobihtml5.com	good	没有服务器地理信息.
service.dcloud.net.cn	good	**IP:** 47.97.36.120 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

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.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://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
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/36199	Android String Resource

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。

向手机申请的权限	是否危险	类型	详细情况
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
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
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: True
Found 1 unique certificates
Subject: C=CN, ST=, L=, O=Android, OU=Android,
CN=yplC7qZE8NuW6LJ105qZDp6NC2v%2Bggiikqb2vncFh4NFGx4T6Zbf7987w8JB6cEbbs7gJFVEqVq4i7oCWK5b%2BeeIg%2B9V4f1pwvjzG7FVmw0%3D
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-12-13 10:51:05+00:00
Valid To: 2121-11-19 10:51:05+00:00
Issuer: C=CN, ST=, L=, O=Android, OU=Android,

CN=yplC7qZE8NuW6LJ105qZDp6NC2v%2Bggiikqb2vncFh4NFGx4T6Zbf7987w8JB6cEbbs7gJFVEqVq4i7oCWK5b%2BeeIg%2B9V4f1pwvjzG7FVmw0%3D
Serial Number: 0x6768a81b
Hash Algorithm: sha256
md5: 4776420960cff8e1189cfa38aa98f801
sha1: 6fe9bdc6704ad1ae32423eca3a062704cc914aeb
sha256: 0fc67540348cb31283c0edff4b10113f6426328bc316b688c5300d9b17ee569a
sha512: 25d8e6e40da151802263fadc83589389c94fb43200a88d2b517519391419765dc8aea6e47074d8bc7df3ef79de6d0f764d8fdfe4beaf7ab107da5a82c6151cd2
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: a7350f6375e423e99c82e203178a0a4d29837c1e7576f1bc0f28d1119b7ea422

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_feature_confusion_exception_no_key_input" : "no public key input"
"dcloud_feature_confusion_exception_no_private_key_input" : "no private key input"
"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"

可能的敏感信息
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_feature_confusion_exception_no_key_input" : "公钥数据为空"
"dcloud_feature_confusion_exception_no_private_key_input" : "私钥数据为空"
"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"

加壳分析

文件列表	分析结果

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.BRAND check Build.PRODUCT check Build.HARDWARE check possible Build.SERIAL check SIM operator check subscriber ID check possible VM check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>
