MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

越好生活 1.0.APK

APP名称:	越好生活
包名:	plus.H5B01A763
域名线索:	7条
URL线索:	36条
邮箱线索:	0条
分析日期:	2022年1月25日 22:59

文件信息

文件名: yuehaoshenghuo582154.apk
文件大小: 3.61MB
MD5值: f77526203c1554f9f97442e1ef15a621
SHA1值: 11a711404a603582af7cab4318a706008e3f894f
SHA256值: 1b4cd2417b1c0e1ee1ee2959f24533575f19bc0fd6e7b5ba0def87329c471d25

APP 信息

App名称: 越好生活
包名: plus.H5B01A763
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 100

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:** 118.31.103.188 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:** 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
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/ad/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/283	io/dcloud/h/b.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/c.java
https://service.dcloud.net.cn/pdz	io/dcloud/f/b/f/a.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/f/b/f/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/f/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/f/a/a.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java

URL信息	Url所在文件
https://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.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

向手机申请的权限	是否危险	类型	详细情况
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.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.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.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_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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.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。
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

向手机申请的权限	是否危险	类型	详细情况
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: False
Found 1 unique certificates
Subject: C=CN, ST=, L=, O=Android, OU=Android,
CN=QJFJIm9UfFTY9wneQjhzXf0WVPh6ne3%2BW4YG0kuuA3qFn2oJb0ageApKVLZhahHuaPXxpq3IcpPqut9JCrdW3w%3D%3D
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2021-08-20 06:08:08+00:00
Valid To: 2121-07-27 06:08:08+00:00
Issuer: C=CN, ST=, L=, O=Android, OU=Android,
CN=QJFJIm9UfFTY9wneQjhzXf0WVPh6ne3%2BW4YG0kuuA3qFn2oJb0ageApKVLZhahHuaPXxpq3IcpPqut9JCrdW3w%3D%3D
Serial Number: 0x4d5b524d
Hash Algorithm: sha256
md5: d18a17d9cb0a7cfacb0bf0b911708782
sha1: f7fedc54a54b61bc387f263275f8bc674a04c45f
sha256: 3ad54b0d3f453b238267cc89ebc075aea64d28f7f4578010c9d3ce6af3f72e29
sha512: 2831e960d96a4bd6cf140e87cbec2f44875b89f1101b0cb5ef8b117d24a52f82063443c771ff144c68a1527f16a0adfc5fbd21ecc86276a228fdbdcc4216375a
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8a0678159778e117afb62b01a59bf633e20e5b5cdfb8b2c8535a73cee52c35c5

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"

可能的敏感信息
"dcloud_permissions_reauthorization" : "重新授权"

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5b01a763://,

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