MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

月牙互动 3.1.8.APK

APP名称:	月牙互动
包名:	io.dcloud.H52AE9AA1
域名线索:	9条
URL线索:	28条
邮箱线索:	0条
分析日期:	2022年2月3日 13:04

文件信息

文件名: yeuyahudong.apk
文件大小: 5.91MB
MD5值: 2a6b8be45cb0a94f8d3af052d22a3026
SHA1值: 3da06ce72cce22fd0005537da05b4cb492a9d2d1
SHA256值: dbfa1b79356a0fd30697181a0cc69ebe751f9782f10d22f1021d81a4ac3a78a5

APP 信息

App名称: 月牙互动
包名: io.dcloud.H52AE9AA1
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 3.1.8
安卓版本: 129

域名线索

域名	是否危险域名	服务器信息
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
stream.mobihtml5.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
update.dcloud.net.cn	good	**IP:** 182.254.52.213 **所属国家:** China **地区:** Guangdong **城市:** Shenzhen **纬度:** 22.545540 **经度:** 114.068298 **查看地图:** Google Map
www.dcloud.io	good	**IP:** 125.37.206.2 **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
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
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
schemas.android.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
streamapp.sinaapp.com	good	**IP:** 127.0.0.1 **所属国家:** - **地区:** - **城市:** - **纬度:** 0.000000 **经度:** 0.000000 **查看地图:** Google Map
ask.dcloud.net.cn	good	**IP:** 222.85.26.227 **所属国家:** China **地区:** Henan **城市:** Zhengzhou **纬度:** 34.757778 **经度:** 113.648613 **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://m3w.cn/sd/reg	io/dcloud/appstream/SideBar.java
http://m3w.cn/s/	io/dcloud/appstream/share/Streamapp_Share.java

URL信息	Url所在文件
http://ask.dcloud.net.cn/article/283	io/dcloud/feature/b.java
https://service.dcloud.net.cn/advert/splash	io/dcloud/feature/ad/a/a.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/common/b/a.java
https://service.dcloud.net.cn/collect/plusapp/action?	io/dcloud/common/util/TestUtil.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://www.dcloud.io/streamapp/streamapp.apk	io/dcloud/common/util/ShortCutUtil.java
http://stream.dcloud.net.cn/resource/sitemap/v2?appid=	io/dcloud/common/a/d.java
https://service.dcloud.net.cn/collect/plusapp/startup	io/dcloud/common/a/d.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
http://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://stream.mobihtml5.com/	io/dcloud/common/constant/StringConst.java
http://update.dcloud.net.cn/apps/	io/dcloud/common/constant/IntentConst.java
http://streamapp.sinaapp.com	io/dcloud/streamdownload/utils/CommitPointData.java

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

向手机申请的权限	是否危险	类型	详细情况
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.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
com.android.launcher.permission.UNINSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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
com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价

向手机申请的权限	是否危险	类型	详细情况
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.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.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.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息

向手机申请的权限	是否危险	类型	详细情况
com.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcherL.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.qiku.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.huawei.android.launcher.permission.READ_SETTINGS	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.zte.mifavor.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lenovo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.google.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.yulong.android.launcher3.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.qihoo360.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.lge.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
net.qihoo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
org.adwfreak.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
org.adw.launcher_donut.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher3.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.fede.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.sec.android.app.twlauncher.settings.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.tencent.qqlauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.huawei.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ebproductions.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.nd.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
com.yulong.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.android.mylauncher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.ztemt.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
cn.nubia.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.gionee.amisystem.permission.READ_SHORTCUT	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=86, ST=贵州, L=贵阳, O=贵州黔贵金服科技有限公司, OU=贵州黔贵金服科技有限公司, CN=qgjf
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-27 06:01:01+00:00
Valid To: 2119-12-03 06:01:01+00:00
Issuer: C=86, ST=贵州, L=贵阳, O=贵州黔贵金服科技有限公司, OU=贵州黔贵金服科技有限公司, CN=qgjf
Serial Number: 0x54af49be

Hash Algorithm: sha256
md5: 0ba443363738254291fab99a30b4e29a
sha1: c09fa5fcc9eaa8fd6f482a1283116ac337aa01a4
sha256: 11ab04073c9a8a08db4b48a8eb2fdcb099a85831314b6e220a7537fefc75160d
sha512: b217abbcfd3b76c9ca2b2ca8c53af5ca94848e503ede230149984ba288b651275d37570931277a3e35ec99dbfd158f44c4fceed09709c27a558c0f3af19eb047
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 88bb436b180fde2cdf0c2b5bb28f58aa881cc8ed46457e6fc4a6a1aaa30b01f0

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntryActivity	Schemes: h52ae9aa1://,

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.PRODUCT check
SIM operator check
device ID check
subscriber ID check
possible VM check</td></tr>
<tr><td>编译器</td><td>dx</td></tr>
</table>
</td></tr>
</table>
