



MoGua

神州智电 1.0.1.APK 分析报告



APP名称:

神州智电

包名:	plus.H569E8560
域名线索:	10条
URL线索:	16条
邮箱线索:	1条
分析日期:	2025年6月25日
分析平台:	摸瓜APK反编译平台

文件名: 神州智电传销.apk
文件大小: 8.65MB
MD5值: c2fbf93ca7493a789efb463fa5a7b13c
SHA1值: f3b4bab0312348b387e84e97065fb9f1fc2d6dbe
SHA256值: c3f2329d1250211fdcf00dfe8532e3dc69ca159161fac5958cdaef7be6a4cd42

i APP 信息

App名称: 神州智电
包名: plus.H569E8560
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.1
安卓版本: 100

🔍 域名线索

域名	服务器信息
er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.
img01.yzcdn.cn	IP: 221.15.70.53 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683289 经度: 112.453911
er.dcloud.net.cn	IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

schemas.android.com	没有服务器地理信息.
m3w.cn	IP: 60.221.17.50 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
bit.ly	IP: 67.199.248.10 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.750134 经度: -73.997009
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
ask.dcloud.net.cn	IP: 101.72.254.86 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717

URL线索

URL信息	Url所在文件
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://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/35058	io/dcloud/feature/audio/AudioRecorderMgr.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

https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://img01.yzcdn.cn/upload_files/2020/06/24/FmKWDg0bN9rMcTp9ne8MXiQWGtLn.png	摸瓜V2引擎
https://bit.ly/2Zqjzkp	摸瓜V2引擎
https://img01.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
https://img01.yzcdn.cn/vant/coupon-empty.png	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.41.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
jhruby.web@gmail.com	摸瓜V2引擎

手机线索

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=, L=, O=Android, OU=Android,
CN=5QOyDik%2FXKC7E8m8%2FxyC64A5KKcedg06lgk%2FRucCPLRh2Oe0%2BJMvolOJPUGP8Y%2BpAGnrNdMGHdHK4bl0LQVVQ%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-22 09:39:10+00:00
有效期至: 2125-03-29 09:39:10+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android,
CN=5QOyDik%2FXKC7E8m8%2FxyC64A5KKcedg06lgk%2FRucCPLRh2Oe0%2BJMvolOJPUGP8Y%2BpAGnrNdMGHdHK4bl0LQVVQ%3D%3D
序列号: 0x5511bf44
哈希算法: sha256
md5值: 3c6fa9ec0b9a8aa72423dbe629709875
sha1值: d1598a0a7dacc302970d9ddc3c3c5019b9d662c4
sha256值: e082b155bf353f2f410a7687424d76db0048f9328ae527a9f1eb0e0e4a25546d
sha512值: 7b5a7105ce0e101faae3c35bc3aa4578d879c04778e8cd89e8a079a7b6d34c4567ea623307b1f1d075215323877cd3791fb3a49530eed120b262f61d85aa0faa
公钥算法: rsa
密钥长度: 2048
指纹: 50736d4f31bd5563be617eed0883a0bc75e18024aca677d84cd57e9d29f83976

 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_tips_certificate" : "certificate"
"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"
"dcloud_tips_certificate" : "证书"

 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_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
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
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.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.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
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h569e8560://,

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。