Evaluation Warning: The document was created with Spire.Doc for Python.

**协同大夫(遂平)（ 2.0.9版本）
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 协同大夫(遂平) |
| 版本 | 2.0.9 |
| 包名 | plus.H5BEE2802 |
| 域名线索 | 77条 |
| URL线索 | 53条 |
| APP图标 |  |
| 分析日期 | 2024年11月7日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | Doctor.apk |
| 文件大小 | 12.06MB |
| MD5值 | 28852264f15f1a0c25792a3cf7020d82 |
| SHA1值 | 2f16a6e6568f76dfbb6bfa525b378c2ca1cd951c |
| SHA256值 | 7ab3a8d8af610a676b3dc81028cbaa6f4b7b3f2dd823868848c5cb3367684abb |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 协同大夫(遂平) |
| 包名 | plus.H5BEE2802 |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 2.0.9 |
| 安卓版本 | 87 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |
| stackoverflow.com | IP: 104.18.32.7 所属国家: United States of America 地区: California 城市: San Francisco  |
| 118.31.238.73 | IP: 118.31.238.73 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| indoorsearch.map.baidu.com | IP: 111.206.209.201 所属国家: China 地区: Beijing 城市: Beijing  |
| suiping.xietongdaifu.com | IP: 218.29.229.70 所属国家: China 地区: Henan 城市: Zhumadian  |
| suipingdownload.xietongdaifu.com | IP: 218.29.229.70 所属国家: China 地区: Henan 城市: Zhumadian  |
| s-gt.getui.com | IP: 124.160.155.61 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| dehealth-test.xietongdaifu.com | IP: 218.29.229.133 所属国家: China 地区: Henan 城市: Zhumadian  |
| mapsv0.bdimg.com | IP: 123.117.133.38 所属国家: China 地区: Beijing 城市: Beijing  |
| www.dcloud.io | IP: 123.6.42.197 所属国家: China 地区: Henan 城市: Zhengzhou  |
| loc.map.baidu.com | IP: 111.206.209.174 所属国家: China 地区: Beijing 城市: Beijing  |
| bugs.webkit.org | IP: 17.253.87.202 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dev.dcloud.net.cn | IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing  |
| bugs.jquery.com | IP: 104.131.8.164 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| mapoffdownload.bdstatic.com | IP: 150.138.157.36 所属国家: China 地区: Shandong 城市: Qingdao  |
| 192.168.1.178 | IP: 192.168.1.178 所属国家: - 地区: - 城市: -  |
| v.map.baidu.com | IP: 111.206.209.185 所属国家: China 地区: Beijing 城市: Beijing  |
| api.map.baidu.com | IP: 111.206.209.166 所属国家: China 地区: Beijing 城市: Beijing  |
| drafts.csswg.org | IP: 45.79.94.155 所属国家: United States of America 地区: California 城市: Fremont  |
| sizzlejs.com | IP: 104.17.98.190 所属国家: United States of America 地区: California 城市: San Francisco  |
| html.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| er.dcloud.net.cn | IP: 43.142.57.168 所属国家: China 地区: Beijing 城市: Beijing  |
| suipingweixin.xietongdaifu.com | IP: 218.29.229.133 所属国家: China 地区: Henan 城市: Zhumadian  |
| bugs.chromium.org | IP: 142.251.211.243 所属国家: United States of America 地区: California 城市: Mountain View  |
| d.gt.igexin.com | 没有服务器地理信息.  |
| errors.angularjs.org | IP: 151.101.65.195 所属国家: United States of America 地区: California 城市: San Francisco  |
| live.xietongdaifu.com | IP: 218.29.229.133 所属国家: China 地区: Henan 城市: Zhumadian  |
| newclient.map.baidu.com | IP: 111.206.209.17 所属国家: China 地区: Beijing 城市: Beijing  |
| j.map.baidu.com | IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing  |
| weixin-test.xietongdaifu.com | IP: 218.29.229.133 所属国家: China 地区: Henan 城市: Zhumadian  |
| ask.dcloud.net.cn | IP: 221.204.43.242 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| bugzilla.mozilla.org | IP: 34.110.178.183 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| daup.map.baidu.com | IP: 110.242.69.98 所属国家: China 地区: Hebei 城市: Baoding  |
| web.archive.org | IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| connect.microsoft.com | IP: 20.112.250.133 所属国家: United States of America 地区: Iowa 城市: Des Moines  |
| app.navi.baidu.com | IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing  |
| ns.adobe.com | 没有服务器地理信息.  |
| 47.97.37.100 | IP: 47.97.37.100 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| 192.168.1.20 | IP: 192.168.1.20 所属国家: - 地区: - 城市: -  |
| 218.29.80.254 | IP: 218.29.80.254 所属国家: China 地区: Henan 城市: Zhengzhou  |
| jquery.org | IP: 104.17.176.200 所属国家: United States of America 地区: California 城市: San Francisco  |
| aui.github.com | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| msdn.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| 218.29.80.252 | IP: 218.29.80.252 所属国家: China 地区: Henan 城市: Zhengzhou  |
| ofloc.map.baidu.com | IP: 111.206.209.193 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weixin.qq.com | IP: 220.196.154.28 所属国家: China 地区: Jiangsu 城市: Wuxi  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| sv.map.baidu.com | IP: 111.206.209.186 所属国家: China 地区: Beijing 城市: Beijing  |
| vectormap0.bdimg.com | IP: 150.138.157.35 所属国家: China 地区: Shandong 城市: Qingdao  |
| client.map.baidu.com | IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing  |
| jsperf.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| newvector.map.baidu.com | IP: 111.206.209.171 所属国家: China 地区: Beijing 城市: Beijing  |
| c-hzgt2.getui.com | IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| schemas.android.com | 没有服务器地理信息.  |
| daohang.map.baidu.com | IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing  |
| 172.20.20.71 | IP: 172.20.20.71 所属国家: - 地区: - 城市: -  |
| sdk.open.phone.igexin.com | IP: 124.160.155.44 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| 172.20.20.70 | IP: 172.20.20.70 所属国家: - 地区: - 城市: -  |
| weixin.xietongdaifu.com | IP: 218.29.229.130 所属国家: China 地区: Henan 城市: Zhumadian  |
| sdk.open.lbs.igexin.com | IP: 121.52.255.89 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| m3w.cn | IP: 60.221.17.65 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| 218.29.80.251 | IP: 218.29.80.251 所属国家: China 地区: Henan 城市: Zhengzhou  |
| itsmap3.baidu.com | IP: 153.37.235.49 所属国家: China 地区: Jiangsu 城市: Xuzhou  |
| er.dcloud.io | 没有服务器地理信息.  |
| offmap2.baidu.com | IP: 61.163.9.35 所属国家: China 地区: Henan 城市: Luoyang  |
| wapmap.baidu.com | IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| promisesaplus.com | IP: 104.21.93.212 所属国家: United States of America 地区: California 城市: San Francisco  |
| angularjs.org | IP: 151.101.1.195 所属国家: United States of America 地区: California 城市: San Francisco  |
| aip.baidubce.com | IP: 111.206.210.12 所属国家: China 地区: Beijing 城市: Beijing  |
| 172.20.22.32 | IP: 172.20.22.32 所属国家: - 地区: - 城市: -  |
| jquery.com | IP: 104.18.156.119 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/e/d.java  |
| https://loc.map.baidu.com/tcu.php  | com/baidu/location/e/d.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/e/d.java  |
| https://loc.map.baidu.com/cfgs/loc/commcfgs  | com/baidu/location/e/d.java  |
| https://client.map.baidu.com/phpui2/?  | com/baidu/location/e/d.java  |
| https://loc.map.baidu.com/cfgs/indoorloc/indoorroadnet  | com/baidu/location/e/d.java  |
| https://loc.map.baidu.com/check\_indoor\_data\_update  | com/baidu/location/e/d.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/e/k.java  |
| https://loc.map.baidu.com/cc.php  | com/baidu/location/b/h.java  |
| https://ofloc.map.baidu.com/locnu  | com/baidu/location/b/x.java  |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/b/j.java  |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| http://daohang.map.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://app.navi.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://map.baidu.com/zt/client/index/?fr=sdk\_[  | com/baidu/mapapi/utils/OpenClientUtil.java  |
| http://api.map.baidu.com/place/detail?uid=  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/place/search?  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/direction?  | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java  |
| https://api.map.baidu.com/lbs\_sdkcc/report  | com/baidu/mapsdkplatform/comapi/b/a/c.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/reverse\_geocoding/v3  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/a.java  |
| http://j.map.baidu.com/  | com/baidu/platform/domain/a.java  |
| http://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather\_abroad/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/parking/search  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/polygon/v1/search  | com/baidu/platform/domain/a.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/detail  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/reverse\_geocoding/v3  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/b.java  |
| https://j.map.baidu.com/  | com/baidu/platform/domain/b.java  |
| https://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/weather\_abroad/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/parking/search  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/polygon/v1/fuzzy\_search  | com/baidu/platform/domain/b.java  |
| http://wapmap.baidu.com/s?tn=Detail&pid=  | com/baidu/platform/core/g/c.java  |
| http://map.baidu.com/?newmap=1&s=  | com/baidu/platform/core/g/e.java  |
| http://sdk.open.phone.igexin.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://c-hzgt2.getui.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://s-gt.getui.com/api.php  | com/igexin/push/config/SDKUrlConfig.java  |
| http://d.gt.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://sdk.open.lbs.igexin.com/api.htm  | com/igexin/push/config/SDKUrlConfig.java  |
| http://bi.  | com/igexin/push/config/n.java  |
| http://config.  | com/igexin/push/config/n.java  |
| http://stat.  | com/igexin/push/config/n.java  |
| http://log.  | com/igexin/push/config/n.java  |
| http://lbs.  | com/igexin/push/config/n.java  |
| http://sdk.open.phone.igexin.com/api/addr.htm  | com/igexin/push/extension/distribution/gbd/d/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://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/e/b/a.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/e/b/a.java  |
| https://er.dcloud.io/rv  | io/dcloud/e/c/h/c.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/e/c/h/c.java  |
| https://ask.dcloud.net.cn/article/285  | io/dcloud/js/map/adapter/BaiduErrorLink.java  |
| https://ask.dcloud.net.cn/article/29  | io/dcloud/js/map/adapter/DHMapView.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/g/b.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://ask.dcloud.net.cn/article/29  | 摸瓜V1引擎  |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_basic?access\_token='  | 摸瓜V2引擎  |
| https://aip.baidubce.com/rest/2.0/ocr/v1/idcard  | 摸瓜V2引擎  |
| http://angularjs.org  | 摸瓜V2引擎  |
| http://errors.angularjs.org/1.4.8/  | 摸瓜V2引擎  |
| http://aui.github.com/artTemplate/\*/  | 摸瓜V2引擎  |
| http://192.168.1.178:8080/h5/';  | 摸瓜V2引擎  |
| http://www.dcloud.io/hellomui/  | 摸瓜V2引擎  |
| http://192.168.1.178:8080/h5/';  | 摸瓜V2引擎  |
| http://www.dcloud.io/hellomui/  | 摸瓜V2引擎  |
| https://github.com/ftlabs/fastclick/issues/251  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=922896  | 摸瓜V2引擎  |
| http://msdn.microsoft.com/en-us/library/windows/apps/Hh767313.aspx  | 摸瓜V2引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| http://api.map.baidu.com/geocoder/v2/';  | 摸瓜V2引擎  |
| http://suiping.xietongdaifu.com/portalb2b  | 摸瓜V2引擎  |
| http://172.20.20.71:8080/portalb2b  | 摸瓜V2引擎  |
| http://suiping.xietongdaifu.com:8080  | 摸瓜V2引擎  |
| http://47.97.37.100:';  | 摸瓜V2引擎  |
| http://172.20.20.70  | 摸瓜V2引擎  |
| http://weixin.xietongdaifu.com/deccpwechat/  | 摸瓜V2引擎  |
| https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx33cad1da23f4a01f&redirect\_uri=http%3a%2f%2fweixin.xietongdaifu.com%2Fdeccpwechat%2Fpage%2Fhtml%2Flive%2FliveIntroduce.html&response\_type=code&scope=snsapi\_base  | 摸瓜V2引擎  |
| http://live.xietongdaifu.com/de-learning  | 摸瓜V2引擎  |
| http://218.29.80.251:8888/portalb2b  | 摸瓜V2引擎  |
| http://218.29.80.251:8080/portalb2b  | 摸瓜V2引擎  |
| http://218.29.80.251:8880  | 摸瓜V2引擎  |
| http://118.31.238.73:';  | 摸瓜V2引擎  |
| http://suipingweixin.xietongdaifu.com/dehealthwechat  | 摸瓜V2引擎  |
| http://218.29.80.251:8080/portalb2c  | 摸瓜V2引擎  |
| http://dehealth-test.xietongdaifu.com/portalb2b  | 摸瓜V2引擎  |
| http://weixin-test.xietongdaifu.com/deccpwechat/  | 摸瓜V2引擎  |
| https://open.weixin.qq.com/connect/oauth2/authorize?appid=wxd2d8f65deb05938e&redirect\_uri=http%3a%2f%2fweixin-test.xietongdaifu.com%2Fdeccpwechat%2Fpage%2Fhtml%2Flive%2FliveIntroduce.html&response\_type=code&scope=snsapi\_base  | 摸瓜V2引擎  |
| https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx991c30651b971883&redirect\_uri=http%3a%2f%2fweixin-test.xietongdaifu.com%2Fdeccpwechat%2Fpage%2Fhtml%2Flive%2FliveIntroduce.html&response\_type=code&scope=snsapi\_base  | 摸瓜V2引擎  |
| http://218.29.80.254:8090/de-learning  | 摸瓜V2引擎  |
| http://172.20.20.71:8880  | 摸瓜V2引擎  |
| http://192.168.1.20:8080/portalb2b  | 摸瓜V2引擎  |
| http://172.20.22.32:8080/Dealeasy-IM  | 摸瓜V2引擎  |
| https://jquery.com/  | 摸瓜V2引擎  |
| https://sizzlejs.com/  | 摸瓜V2引擎  |
| https://jquery.org/license  | 摸瓜V2引擎  |
| https://github.com/eslint/eslint/issues/6125  | 摸瓜V2引擎  |
| http://jquery.org/license  | 摸瓜V2引擎  |
| https://jsperf.com/thor-indexof-vs-for/5  | 摸瓜V2引擎  |
| https://drafts.csswg.org/cssom/  | 摸瓜V2引擎  |
| https://bugs.jquery.com/ticket/13378  | 摸瓜V2引擎  |
| https://bugs.jquery.com/ticket/12359  | 摸瓜V2引擎  |
| https://msdn.microsoft.com/en-us/library/ie/hh465388.aspx  | 摸瓜V2引擎  |
| https://bugs.webkit.org/show\_bug.cgi?id=136851  | 摸瓜V2引擎  |
| https://github.com/jquery/sizzle/pull/225  | 摸瓜V2引擎  |
| https://msdn.microsoft.com/en-us/library/ms536429%28VS.85%29.aspx  | 摸瓜V2引擎  |
| https://promisesaplus.com/  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=378607  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=470258  | 摸瓜V2引擎  |
| https://github.com/eslint/eslint/issues/3229  | 摸瓜V2引擎  |
| https://connect.microsoft.com/IE/feedback/details/1736512/  | 摸瓜V2引擎  |
| https://jsperf.com/getall-vs-sizzle/2  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/CSS/display  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=649285  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=491668  | 摸瓜V2引擎  |
| https://web.archive.org/web/20100324014747/http://blindsignals.com/index.php/2009/07/jquery-delay/  | 摸瓜V2引擎  |
| https://web.archive.org/web/20141116233347/http://fluidproject.org/blog/2008/01/09/getting-setting-and-removing-tabindex-values-with-javascript/  | 摸瓜V2引擎  |
| https://html.spec.whatwg.org/  | 摸瓜V2引擎  |
| https://bugzilla.mozilla.org/show\_bug.cgi?id=687787  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=449857  | 摸瓜V2引擎  |
| http://example.com:80x/  | 摸瓜V2引擎  |
| https://bugs.webkit.org/show\_bug.cgi?id=137337  | 摸瓜V2引擎  |
| https://bugs.webkit.org/show\_bug.cgi?id=29084  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=589347  | 摸瓜V2引擎  |
| https://github.com/jrburke/requirejs/wiki/Updating-existing-libraries  | 摸瓜V2引擎  |
| https://github.com/jquery/jquery/pull/557)  | 摸瓜V2引擎  |
| http://dev.dcloud.net.cn/mui)  | 摸瓜V2引擎  |
| https://github.com/joewalnes/reconnecting-websocket/  | 摸瓜V2引擎  |
| http://stackoverflow.com/questions/19345392/why-arent-my-parameters-getting-passed-through-to-a-dispatched-event/19345563  | 摸瓜V2引擎  |
| http://suipingdownload.xietongdaifu.com:8080/update';  | 摸瓜V2引擎  |
| http://218.29.80.252:88/update  | 摸瓜V2引擎  |
| http://github.com/brix/crypto-js  | 摸瓜V2引擎  |
| http://github.com/brix/crypto-js.git  | 摸瓜V2引擎  |
| http://github.com/evanvosberg  | 摸瓜V2引擎  |
| http://github.com/brix/crypto-js  | 摸瓜V2引擎  |
| http://github.com/brix/crypto-js.git  | 摸瓜V2引擎  |
| http://dev.dcloud.net.cn/mui)  | 摸瓜V2引擎  |
| http://dev.dcloud.net.cn/mui)  | 摸瓜V2引擎  |
| http://api.map.baidu.com/geocoder/v2/';  | 摸瓜V2引擎  |
| https://newclient.map.baidu.com/client/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://client.map.baidu.com/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://v.map.baidu.com/low/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://v.map.baidu.com/indoorinside/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://v.map.baidu.com/high/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newclient.map.baidu.com/pic/newvector/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newvector.map.baidu.com/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://vectormap0.bdimg.com/vecdata/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newclient.map.baidu.com/its/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://itsmap3.baidu.com/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newvector.map.baidu.com/starpic/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://client.map.baidu.com/heatmap/client?  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://sv.map.baidu.com  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://sv.map.baidu.com/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://client.map.baidu.com/offline-search/?  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://offmap2.baidu.com/offline-search/?  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://mapoffdownload.bdstatic.com/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newvector.map.baidu.com/grid\_vc/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newclient.map.baidu.com/pic/newvector/topic\_map/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://newvector.map.baidu.com/travel\_vc/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://indoorsearch.map.baidu.com/is/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://mapsv0.bdimg.com/?  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://client.map.baidu.com/imap/sdk/tj?qt=vmap  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/statistics/v1/  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=  | lib/armeabi-v7a/libBaiduMapSDK\_map\_v7\_5\_3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 1228joes@163.com  | 摸瓜V2引擎  |
| houfeng@dcloud.io  | 摸瓜V2引擎  |
| houfeng@dcloud.io  | 摸瓜V2引擎  |
| houfeng@dcloud.io  | 摸瓜V2引擎  |
| houfeng@dcloud.io  | 摸瓜V2引擎  |
| houfeng@dcloud.io  | 摸瓜V2引擎  |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |
| jhruby.web@gmail.com  | 摸瓜V2引擎  |
| cuihongbao@dcloud.io  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118  | com/baidu/mapsdkplatform/comapi/util/b.java  |
| 15418662026  | com/igexin/push/extension/distribution/gbd/i/a/b.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=86, ST=北京, L=海淀, O=数字天堂（北京）网络技术有限公司, OU=数字天堂（北京）网络技术有限公司, CN=DH 签名算法: rsassa\_pkcs1v15 有效期自: 2013-04-22 06:45:31+00:00 有效期至: 3012-08-23 06:45:31+00:00 发行人: C=86, ST=北京, L=海淀, O=数字天堂（北京）网络技术有限公司, OU=数字天堂（北京）网络技术有限公司, CN=DH 序列号: 0x5174dc8b 哈希算法: sha1 md5值: 59201cf6589202cb2cdab26752472112 sha1值: baad093a82829fb432a7b28cb4ccf0e9f37dae58 sha256值: d75c1fa2b9ae867ce688a8adc6deac7cd6ba96f43a751fd10a200fa5974ac636 sha512值: 16a37ece684bec4a3608fd375cd189eecd78eb7163a3afd1654225148e71ae07cce7755c0a9e8466dd4be505d526c19f7340a2040bd3f43004081ea409f70146 公钥算法: rsa 密钥长度: 1024 指纹: 426f7db3074401182137b947e553230a7e4c1801f824985f9fce57d65753f781**

## **6. 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"  |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看  |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看  |  |  |

## **9. 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。 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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 |
| 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 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| 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 |
| 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 |
| 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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| getui.permission.GetuiService.plus.H5BEE2802 | 未知 | Unknown permission | Unknown permission from android reference |
| 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.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| com.asus.msa.SupplementaryDID.ACCESS | 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\_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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.PandoraEntry | **Schemes**: h5bee2802://,  |

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