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

**CrowdMag（ 2.2.1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 | CrowdMag |
| 版本 | 2.2.1 |
| 包名 | gov.noaa.ngdc.wmm2 |
| 域名线索 | 8条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年8月15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 | CrowdMag\_2.2.1\_APKPure.apk |
| 文件大小 | 11.5MB |
| MD5值 | f0e7b817a674868fbf33c619d6852eae |
| SHA1值 | f41d903374cae4552b40068a6a98b57da494dc6b |
| SHA256值 | 5e43e7029949e8439ae346aa64c9492ab0f477bc187050a60c9f4a46fe69f14f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | CrowdMag |
| 包名 | gov.noaa.ngdc.wmm2 |
| 主活动Activity | gov.noaa.ngdc.wmm2.MainActivity |
| 安卓版本名称 | 2.2.1 |
| 安卓版本 | 162 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.jjoe64.com | 没有服务器地理信息.  |
| services.swpc.noaa.gov | IP: 99.86.195.78 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| go.usa.gov | IP: 13.226.225.61 所属国家: United States of America 地区: California 城市: Los Angeles  |
| forms.gle | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.ncei.noaa.gov | IP: 205.167.25.171 所属国家: United States of America 地区: North Carolina 城市: Asheville  |
| www.gnu.org | IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville  |
| www.ngdc.noaa.gov | IP: 140.172.190.2 所属国家: United States of America 地区: Colorado 城市: Boulder  |
| noaa.maps.arcgis.com | IP: 3.224.213.48 所属国家: United States of America 地区: Virginia 城市: Ashburn  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.ngdc.noaa.gov/crowdmag/flight\_measurements  | gov/noaa/ngdc/wmm/crowdmag/util/ReportingService.java  |
| https://www.ngdc.noaa.gov/crowdmag/measurements  | gov/noaa/ngdc/wmm/crowdmag/util/ReportingService.java  |
| https://www.ngdc.noaa.gov/geomag/crowdmag/mobilemessage.json  | gov/noaa/ngdc/wmm/crowdmag/util/RecordingService.java  |
| https://noaa.maps.arcgis.com/apps/instant/slider/index.html?appid=37da82c22ecf4a51b9acefa5309f9872  | gov/noaa/ngdc/wmm/fragments/CrowdMagFragment.java  |
| https://forms.gle/hihRqhYXwiVq8UE8A  | gov/noaa/ngdc/wmm/fragments/CrowdMagFragment.java  |
| http://go.usa.gov/3q3aH  | gov/noaa/ngdc/wmm/fragments/CrowdMagFragment.java  |
| https://services.swpc.noaa.gov/text/daily-geomagnetic-indices.txt  | gov/noaa/ngdc/wmm/fragments/CompassFragment.java  |
| https://www.ncei.noaa.gov/products/crowdmag/tutorial  | gov/noaa/ngdc/wmm/fragments/SettingsFragment.java  |
| https://www.ncei.noaa.gov/products/crowdmag-magnetic-data/privacy-policy  | gov/noaa/ngdc/wmm/fragments/SettingsFragment.java  |
| https://www.ngdc.noaa.gov/geomag/WMM/data/MIL-PRF-89500B.pdf).  | gov/noaa/ngdc/wmm/fragments/WMMFragment.java  |
| https://www.ncei.noaa.gov/products/world-magnetic-model/accuracy-limitations-error-model)  | gov/noaa/ngdc/wmm/fragments/WMMFragment.java  |
| https://www.ncei.noaa.gov/products/crowdmag/flight-mode-tutorial  | gov/noaa/ngdc/wmm/fragments/MyDataFragment.java  |
| https://www.ncei.noaa.gov/products/crowdmag/tutorial  | gov/noaa/ngdc/wmm/fragments/MyDataFragment.java  |
| http://go.usa.gov/3q3aH  | gov/noaa/ngdc/wmm/fragments/MyDataFragment.java  |
| http://www.ngdc.noaa.gov/geomag/crowdmag.shtml  | 摸瓜V1引擎  |
| https://www.ngdc.noaa.gov/geomag/crowdmag/mobilemessage.json  | 摸瓜V3引擎  |
| https://www.ngdc.noaa.gov/geomag/WMM/data/MIL-PRF-89500B.pdf).  | 摸瓜V3引擎  |
| http://www.ngdc.noaa.gov/geomag/crowdmag.shtml  | 摸瓜V3引擎  |
| https://services.swpc.noaa.gov/text/daily-geomagnetic-indices.txt  | 摸瓜V3引擎  |
| http://go.usa.gov/3q3aH  | 摸瓜V3引擎  |
| infinitedata-pa.googleapis.com  | 摸瓜V3引擎  |
| http://www.jjoe64.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://www.gnu.org/licenses/lgpl.html  | 摸瓜V3引擎  |
| https://www.ncei.noaa.gov/products/crowdmag/flight-mode-tutorial  | 摸瓜V3引擎  |
| https://forms.gle/hihRqhYXwiVq8UE8A  | 摸瓜V3引擎  |
| play.googleapis.com  | 摸瓜V3引擎  |
| https://www.ngdc.noaa.gov/crowdmag/flight\_measurements  | 摸瓜V3引擎  |
| www.googleapis.com  | 摸瓜V3引擎  |
| https://noaa.maps.arcgis.com/apps/instant/slider/index.html?appid=37da82c22ecf4a51b9acefa5309f9872  | 摸瓜V3引擎  |
| https://www.ncei.noaa.gov/products/crowdmag/tutorial  | 摸瓜V3引擎  |
| https://www.ncei.noaa.gov/products/crowdmag-magnetic-data/privacy-policy  | 摸瓜V3引擎  |
| https://www.ncei.noaa.gov/products/world-magnetic-model/accuracy-limitations-error-model  | 摸瓜V3引擎  |
| https://www.ngdc.noaa.gov/crowdmag/measurements  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| geomag.models@noaa.gov  | gov/noaa/ngdc/wmm/fragments/SettingsFragment.java  |

### **4.4 手机号线索**

## **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: CN=Nir Boneh 签名算法: rsassa\_pkcs1v15 有效期自: 2014-06-02 17:47:48+00:00 有效期至: 2039-05-27 17:47:48+00:00 发行人: CN=Nir Boneh 序列号: 0x50337384 哈希算法: sha256 md5值: 74e47d06265b34f6e4add50ddf34e336 sha1值: 42e134333d3fdb8f9c195f5b0e2cb69970d09fb6 sha256值: d5f2b48e80c171597a31e092eea0481a0af8aa9cb807bb99066f9c11b98d9448 sha512值: e51c4e495974f1220feffa9a162e6b37e0761083fba86bdc24ee9543a955a5fafef79784be5ac3122d099101d68b8429cdf81c1675e21d50bcfe08dd95b6a4f6 公钥算法: rsa 密钥长度: 2048 指纹: a018c2c94c0f07e142e63dae107f2f1b18d9fbbfdfd038d7c74544239c7fab6c**

## **6. 硬编码敏感信息**

## **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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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 |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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 |
| gov.noaa.ngdc.wmm2.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**