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

**PlanetWatch（ 1.5.1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 | PlanetWatch |
| 版本 | 1.5.1 |
| 包名 | io.planetwatch.app |
| 域名线索 | 29条 |
| URL线索 | 36条 |
| APP图标 |  |
| 分析日期 | 2025年6月3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 | PlanetWatch\_1.5.1\_APKPure.apk |
| 文件大小 | 31.08MB |
| MD5值 | db76aa752dfcdf94f172b1315d8b6bb0 |
| SHA1值 | f6534ef284fdaa19bdd4feddca4cbc687caecdd5 |
| SHA256值 | c0d081f52cb17ca514b04ec52f9c3b05d010b576ce2e4dcf5747a3b3fbafbf2f |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | PlanetWatch |
| 包名 | io.planetwatch.app |
| 主活动Activity | io.planetwatch.app.ui.splash.SplashScrActivity |
| 安卓版本名称 | 1.5.1 |
| 安卓版本 | 11333 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| app-measurement.com | IP: 114.250.65.33 所属国家: China 地区: Beijing 城市: Beijing  |
| www.tensorflow.org | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| explorer.planetwatch.io | IP: 13.37.116.247 所属国家: France 地区: Ile-de-France 城市: Paris  |
| firebase.google.com | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| mobileapi.planetwatch.io | IP: 13.39.52.33 所属国家: France 地区: Ile-de-France 城市: Paris  |
| www.iubenda.com | IP: 143.244.50.82 所属国家: United States of America 地区: California 城市: Los Angeles  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| planetwatch.io | IP: 35.71.176.152 所属国家: United States of America 地区: Washington 城市: Seattle  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| plus.google.com | IP: 199.59.150.44 所属国家: United States of America 地区: California 城市: San Francisco  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.planetwatch.io | IP: 104.18.13.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| support.planetwatch.io | 没有服务器地理信息.  |
| app-mobile-3855a.firebaseio.com | IP: 34.120.160.131 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| www.google.com | IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| schemas.android.com | 没有服务器地理信息.  |
| goo.gl | IP: 142.251.215.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| firebase-settings.crashlytics.com | IP: 114.250.69.34 所属国家: China 地区: Beijing 城市: Beijing  |
| pagead2.googlesyndication.com | IP: 114.250.65.38 所属国家: China 地区: Beijing 城市: Beijing  |
| aomedia.org | IP: 4.78.139.54 所属国家: United States of America 地区: New Jersey 城市: Newark  |
| schemas.microsoft.com | IP: 104.212.68.35 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| 192.168.4.1 | IP: 192.168.4.1 所属国家: - 地区: - 城市: -  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| exoplayer.dev | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.googleadservices.com | IP: 114.250.64.38 所属国家: China 地区: Beijing 城市: Beijing  |
| developer.apple.com | IP: 17.253.87.204 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| verify.synaps.io | IP: 104.18.29.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| a044386b30806479b8d0b566643bcb9f-dbd011f34e25fdfc.elb.eu-west-3.amazonaws.com | IP: 13.39.52.33 所属国家: France 地区: Ile-de-France 城市: Paris  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://support.planetwatch.io/hc/en-gb  | io/planetwatch/app/ui/home/learn/LearnFragment.java  |
| https://explorer.planetwatch.io/  | io/planetwatch/app/ui/home/learn/LearnFragment.java  |
| https://planetwatch.io/  | io/planetwatch/app/ui/home/learn/LearnFragment.java  |
| https://www.planetwatch.io/white-paper/index-h5.html  | io/planetwatch/app/ui/home/learn/LearnFragment.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | p000/in6.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | p000/ic4.java  |
| https://plus.google.com/  | p000/oz9.java  |
| https://mobileapi.planetwatch.io/api/algorandnode  | p000/as0.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | p000/xn1.java  |
| http://schemas.android.com/apk/res/android  | p000/yl6.java  |
| https://aomedia.org/emsg/ID3  | p000/im1.java  |
| https://developer.apple.com/streaming/emsg-id3  | p000/im1.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | p000/hi2.java  |
| https://verify.synaps.io/?session\_id=  | p000/z36.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | p000/jd7.java  |
| https://app-measurement.com/a  | p000/zs9.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | p000/hb4.java  |
| https://goo.gl/J1sWQy  | p000/kb8.java  |
| https://x</LA\_URL>  | p000/f32.java  |
| https://x  | p000/f32.java  |
| https://goo.gl/NAOOOI.  | p000/ik9.java  |
| https://goo.gl/NAOOOI  | p000/ik9.java  |
| https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s  | p000/ik9.java  |
| https://mobileapi.planetwatch.io/api/  | p000/ag.java  |
| https://192.168.4.1  | p000/ag.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | p000/qi2.java  |
| https://firebase.google.com/support/privacy/init-options.  | p000/zv1.java  |
| https://app-measurement.com/a  | p000/a88.java  |
| http://ns.adobe.com/xap/1.0/  | p000/vx2.java  |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings  | p000/io5.java  |
| http://dashif.org/guidelines/last-segment-number  | p000/uz0.java  |
| http://dashif.org/guidelines/trickmode  | p000/uz0.java  |
| https://google.com/search?  | p000/p09.java  |
| https://www.google.com  | p000/b19.java  |
| https://firebase.google.com/support/guides/disable-analytics  | p000/x88.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | p000/kr5.java  |
| https://app-mobile-3855a.firebaseio.com  | 摸瓜V1引擎  |
| https://planetwatch.io  | 摸瓜V1引擎  |
| https://www.planetwatch.io/pick-your-license/  | 摸瓜V1引擎  |
| https://www.iubenda.com/privacy-policy/50316447  | 摸瓜V1引擎  |
| https://support.planetwatch.io/hc/en-gb  | 摸瓜V1引擎  |
| https://planetwatch.io/planetwatch-terms-and-conditions-app/  | 摸瓜V1引擎  |
| mobileapi.planetwatch.io  | 摸瓜V3引擎  |
| a044386b30806479b8d0b566643bcb9f-dbd011f34e25fdfc.elb.eu-west-3.amazonaws.com  | 摸瓜V3引擎  |
| firebase-settings.crashlytics.com  | 摸瓜V3引擎  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/arm64-v8a/libbarhopper\_v3.so  |
| http://http  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/arm64-v8a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| http://http  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86/libbarhopper\_v3.so  |
| http://http  | lib/x86/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_select  | lib/x86\_64/libbarhopper\_v3.so  |
| http://http  | lib/x86\_64/libbarhopper\_v3.so  |
| https://www.tensorflow.org/lite/guide/ops\_custom  | lib/x86\_64/libbarhopper\_v3.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | p000/f29.java  |
| android-sdk-releaser@vopo7.prod  | lib/arm64-v8a/libbarhopper\_v3.so  |
| android-sdk-releaser@vopo7.prod  | lib/armeabi-v7a/libbarhopper\_v3.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86/libbarhopper\_v3.so  |
| android-sdk-releaser@vopo7.prod  | lib/x86\_64/libbarhopper\_v3.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869183  | org/msgpack/core/MessageUnpacker.java  |
| 17512775099  | p000/gw.java  |
| 15552000000  | p000/h19.java  |

## **5. 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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-29 09:03:02+00:00 有效期至: 2051-10-29 09:03:02+00:00 发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android 序列号: 0xc5cb94f17deca3ca009ad2fda93fd40c20bf66e2 哈希算法: sha256 md5值: de79cf616ca30bfbf5254a4c30cf7b6c sha1值: aa32a037dc8c011f6c3f40e0d155c0f3162368aa sha256值: e9c6e8f43fa3db670912080abbdbec10a71e33703037e6ea44e86779b106ce01 sha512值: 49f11c8f26fa0994f00f7f9bea54e88dc153303ed2baf81c0b0ec9bbb1c0a099a969e5b8d5b3ec0451038103430949fb3a8d88a73ce36ba74dd98231cffb4394 公钥算法: rsa 密钥长度: 4096 指纹: caa83b9683936ce66e35287996fafa7d846f3d18109938bea965432fc20b130c**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "already\_register\_user" : "Your email is already registered, please go in the login section. If you don't remember your password use the Forgot your password? link. In other cases open a ticket to the Support"  |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "59de2a07c42149c2bbc0ba442f339801"  |
| "enable\_biometric\_auth\_popup\_cancel" : "Not now"  |
| "enable\_biometric\_auth\_popup\_ok" : "OK"  |
| "firebase\_database\_url" : "https://app-mobile-3855a.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyAOr4KrRWIj4BqqRs-QcWClwhQ3QI0RTaI"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAOr4KrRWIj4BqqRs-QcWClwhQ3QI0RTaI"  |
| "insert\_wifi\_password" : "Insert WiFi Password"  |
| "insert\_your\_token" : "Insert your token"  |
| "license\_type\_3\_token\_info" : "Go to the Kaiterra dashboard, click on Your Account, go to Account Settings, generate API Key and then copy the key"  |
| "password" : "Password"  |
| "reset\_password" : "Reset Password"  |
| "set\_password" : "Set Password"  |
| "token" : "Token"  |
| "unchanged\_password" : "The new password must be different from the old one"  |
| "username" : "Username:"  |
| "vote\_token" : "%1$d voting tokens will be sent to your wallet"  |
| "wifi\_password" : "WiFi Password"  |

## **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\_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 | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.USE\_BIOMETRIC | 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.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.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.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| 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。  |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.planetwatch.app.ui.splash.SplashScrActivity | **Schemes**: planetwatch://, **Hosts:** synaps,  |
| net.openid.appauth.RedirectUriReceiverActivity | **Schemes**: planetwatch://app://,  |

**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。**