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

**动物世界（ 1.1.7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 | 动物世界 |
| 版本 | 1.1.7 |
| 包名 | com.hainansd.dwsj |
| 域名线索 | 18条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年7月4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 | neilaxin.apk |
| 文件大小 | 79.01MB |
| MD5值 | be68cb9107110fab01e48dfef122ac4b |
| SHA1值 | 9ff2fa2b9d17cf97e73ece7dc8b11eab0f6234cd |
| SHA256值 | 67de55ee7359d11c1a33c6585b2291d85e1b2fcd2d9abf6eb4d9f0c101de99e1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 动物世界 |
| 包名 | com.hainansd.dwsj |
| 主活动Activity | com.hainansd.dwsj.business.splash.SplashActivity |
| 安卓版本名称 | 1.1.7 |
| 安卓版本 | 1170 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| heycam.github.io | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| www.apple.com | IP: 210.192.117.229 所属国家: China 地区: Beijing 城市: Beijing  |
| www.khronos.org | IP: 104.22.23.137 所属国家: United States of America 地区: California 城市: San Francisco  |
| mon.toutiao.com | IP: 106.117.213.109 所属国家: China 地区: Hebei 城市: Tangshan  |
| mon.toutiaocloud.net | IP: 106.117.244.231 所属国家: China 地区: Hebei 城市: Tangshan  |
| monsetting.toutiao.com | IP: 106.117.244.228 所属国家: China 地区: Hebei 城市: Tangshan  |
| eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| dom.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| mon.toutiaocloud.com | IP: 106.117.213.114 所属国家: China 地区: Hebei 城市: Tangshan  |
| www.saxproject.org | IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego  |
| crbug.com | IP: 216.239.32.29 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.w3.org | IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| cdn.jsdelivr.net | IP: 151.101.109.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| purl.eligrey.com | IP: 104.236.163.66 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.cocos.com | IP: 124.239.250.34 所属国家: China 地区: Hebei 城市: Langfang  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| mon.snssdk.com | IP: 182.254.48.192 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| www.openssl.org | IP: 184.27.21.43 所属国家: Japan 地区: Tokyo 城市: Tokyo  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://eligrey.com  | Mogua Engine V2  |
| https://github.com/dsamarin  | Mogua Engine V2  |
| https://github.com/eligrey/Blob.js/blob/master/LICENSE.md  | Mogua Engine V2  |
| http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml  | Mogua Engine V2  |
| https://dom.spec.whatwg.org/  | Mogua Engine V2  |
| https://heycam.github.io/webidl/  | Mogua Engine V2  |
| https://github.com/taylorhakes  | Mogua Engine V2  |
| https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE  | Mogua Engine V2  |
| https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js  | Mogua Engine V2  |
| http://www.cocos.com  | Mogua Engine V2  |
| https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB\_texture\_float.txt  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml';  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace';  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html  | Mogua Engine V2  |
| http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html  | Mogua Engine V2  |
| http://www.w3.org/TR/REC-DOM-Level-1/ecma-script-language-binding.html  | Mogua Engine V2  |
| http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/ecma-script-binding.html  | Mogua Engine V2  |
| http://www.w3.org/TR/2000/REC-DOM-Level-2-Core-20001113/core.html  | Mogua Engine V2  |
| http://www.w3.org/TR/REC-DOM-Level-1/level-one-core.html  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/')  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml')  | Mogua Engine V2  |
| http://www.w3.org/1999/xhtml'  | Mogua Engine V2  |
| http://www.w3.org/2000/xmlns/';  | Mogua Engine V2  |
| http://www.cocos.com  | Mogua Engine V2  |
| https://www.cocos.com/  | Mogua Engine V2  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/armeabi-v7a/libcocos2djs.so  |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libcocos2djs.so  |
| https://crbug.com/v8/8520  | lib/armeabi-v7a/libcocos2djs.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |
| https://mon.snssdk.com/monitor/appmonitor/v2/settings  | lib/armeabi-v7a/libmetasec\_ml.so  |
| https://monsetting.toutiao.com/monitor/appmonitor/v2/settings  | lib/armeabi-v7a/libmetasec\_ml.so  |
| https://mon.snssdk.com/monitor/collect  | lib/armeabi-v7a/libmetasec\_ml.so  |
| https://mon.toutiao.com/monitor/collect  | lib/armeabi-v7a/libmetasec\_ml.so  |
| https://mon.toutiaocloud.com/monitor/collect  | lib/armeabi-v7a/libmetasec\_ml.so  |
| https://mon.toutiaocloud.net/monitor/collect  | lib/armeabi-v7a/libmetasec\_ml.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/arm64-v8a/libcocos2djs.so  |
| https://www.openssl.org/docs/faq.html  | lib/arm64-v8a/libcocos2djs.so  |
| https://crbug.com/v8/8520  | lib/arm64-v8a/libcocos2djs.so  |
| https://mon.snssdk.com/monitor/appmonitor/v2/settings  | lib/arm64-v8a/libmetasec\_ml.so  |
| https://monsetting.toutiao.com/monitor/appmonitor/v2/settings  | lib/arm64-v8a/libmetasec\_ml.so  |
| https://mon.snssdk.com/monitor/collect  | lib/arm64-v8a/libmetasec\_ml.so  |
| https://mon.toutiao.com/monitor/collect  | lib/arm64-v8a/libmetasec\_ml.so  |
| https://mon.toutiaocloud.com/monitor/collect  | lib/arm64-v8a/libmetasec\_ml.so  |
| https://mon.toutiaocloud.net/monitor/collect  | lib/arm64-v8a/libmetasec\_ml.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| xo@iek.g0m  | Mogua Engine V2  |
| r9xl@m.nz nm3@r.tag smh@idvբ.rg zj@pk.ԗa  | Mogua Engine V2  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |
| cocos@cocoss-macbook-pro.local  | lib/armeabi-v7a/libcocos2djs.so  |
| ffmpeg-devel@ffmpeg.org  | lib/arm64-v8a/libijkplayer.so  |
| cocos@cocoss-macbook-pro.local  | lib/arm64-v8a/libcocos2djs.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates Subject: C=86, ST=BeiJing, L=BeiJing, O=China, CN=CooHua Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2014-04-26 14:26:22+00:00 Valid To: 2114-04-02 14:26:22+00:00 Issuer: C=86, ST=BeiJing, L=BeiJing, O=China, CN=CooHua Serial Number: 0x535bc20e Hash Algorithm: sha1 md5: 830887854b8795f643efcf10b4a0e9d8 sha1: 374da96bc1924bb7268eacfc3ddd7ce500b5ccb5 sha256: 869496b92d7637dfee26900f09462afc7e96c72705f8f69176914bf217bc3069 sha512: 1d902895281e3ec40ca9b13769d9f51c115f2ea350cc6546ff21ff4df6eae05edcfc856880a9441f4c09460801a70f62375c5c2580c6f06e7fd3cf72cc7dcf2d PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: 22e1d14e3031d6b6be18a9b20f4eaf0a7a03284efd4ad8a82bfa15fe1172a0fd**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "str\_tips\_token" : "重要提示"  |
| "str\_token\_expired" : "登录已过期或无效用户，试试重新登录吧~"  |

## **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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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.miui.systemAdSolution.adSwitch.PROVIDER | 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.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.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.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.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.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\_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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.hainansd.dwsj.openadsdk.permission.TT\_PANGOLIN | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.PACKAGE\_USAGE\_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| com.hainansd.dwsj.permission.KW\_SDK\_BROADCAST | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| com.hihonor.permission.MANAGE\_FOLD\_SCREEN | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.permission.MANAGE\_FOLD\_SCREEN\_PRIVILEGED | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.huawei.openalliance.ad.activity.PPSLauncherActivity | **Schemes**: hwpps://, **Hosts:** com.hainansd.dwsj,  |

**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。**