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

**爱威奶（ 7.9.3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 | 爱威奶 |
| 版本 | 7.9.3 |
| 包名 | com.avnight |
| 域名线索 | 33条 |
| URL线索 | 26条 |
| APP图标 |  |
| 分析日期 | 2025年6月18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 | 7\_9\_3\_night.apk |
| 文件大小 | 30.01MB |
| MD5值 | 2377c80ffe56e0ac516b848397b03b12 |
| SHA1值 | f0230aec09841ef495cc83cd9c444a7aaed1af14 |
| SHA256值 | 303f0c0ee5ead2e88716a71dde9314a37f431b8626dad5256404c541cebf8909 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 爱威奶 |
| 包名 | com.avnight |
| 主活动Activity | com.avnight.Activity.LandingActivity.LandingActivity |
| 安卓版本名称 | 7.9.3 |
| 安卓版本 | 293 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| exoplayer.dev | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| schemas.xmlsoap.org | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| java.sun.com | IP: 23.210.26.6 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| android.googlesource.com | IP: 142.251.188.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.mzitu.com | IP: 118.184.78.78 所属国家: China 地区: Shanghai 城市: Shanghai  |
| goo.gl | IP: 74.125.135.102 所属国家: United States of America 地区: California 城市: Mountain View  |
| av9av9-1309454273.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.186 所属国家: China 地区: Fujian 城市: Fuzhou  |
| www.google.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.sec.co.kr | IP: 112.106.187.200 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| av9av9-1318371851.cos.accelerate.myqcloud.com | IP: 111.202.29.114 所属国家: China 地区: Beijing 城市: Beijing  |
| bitdash-a.akamaihd.net | IP: 2.19.117.147 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: London  |
| firebase-settings.crashlytics.com | IP: 114.250.67.34 所属国家: China 地区: Beijing 城市: Beijing  |
| av9av9-1318371851.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.185 所属国家: China 地区: Fujian 城市: Fuzhou  |
| dev-avnight-cpi.appdev.icu | IP: 139.162.98.177 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| qlaops.nongchang168.com | 没有服务器地理信息.  |
| glassfish.dev.java.net | IP: 137.254.56.48 所属国家: United States of America 地区: California 城市: Belmont  |
| storage.googleapis.com | IP: 142.250.107.207 所属国家: United States of America 地区: California 城市: Mountain View  |
| a9-cos.dango33.com | IP: 103.199.103.112 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| app-av9-8631e.firebaseio.com | IP: 35.201.97.85 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| ns.adobe.com | 没有服务器地理信息.  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| pv.sohu.com | IP: 124.163.195.89 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| 9ynefxy-1.sbs | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| i.imgur.com | IP: 103.228.130.27 所属国家: Spain 地区: Valenciana, Comunidad 城市: Alicante  |
| d1vcfwitp2um8b.cloudfront.net | IP: 65.9.37.120 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| aomedia.org | IP: 74.86.228.110 所属国家: United States of America 地区: California 城市: San Jose  |
| openinstall.iavnight.com | IP: 162.125.32.10 所属国家: United States of America 地区: California 城市: San Francisco  |
| 9cl.yangguanging.com | 没有服务器地理信息.  |
| www.google-analytics.com | IP: 114.250.70.33 所属国家: China 地区: Beijing 城市: Beijing  |
| default.url | 没有服务器地理信息.  |
| api.api98.xyz | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://av9av9-1309454273.cos.ap-guangzhou.myqcloud.com/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://av9av9-1318371851.cos.ap-guangzhou.myqcloud.com/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://storage.googleapis.com/a9a9/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://d1vcfwitp2um8b.cloudfront.net/api/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://a9-cos.dango33.com/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://av9av9-1318371851.cos.accelerate.myqcloud.com/host\_and.jsonb  | com/avnight/Activity/LandingActivity/p0.java  |
| https://openinstall.iavnight.com/api/  | com/avnight/Activity/LandingActivity/r0.java  |
| https://www.mzitu.com/  | com/avnight/Activity/MaituViewerActivity/u.java  |
| https://www.mzitu.com/  | com/avnight/Activity/MaituViewerActivity/v.java  |
| https://bitdash-a.akamaihd.net/content/sintel/hls/video/  | com/avnight/Activity/VideoStorageActivity/c0.java  |
| https://www.google-analytics.com/mp/collect?measurement\_id=  | com/avnight/EventTracker/MeasurementGA.java  |
| https://i.imgur.com/TOo1GxX.jpeg  | com/avnight/ApiModel/AvVideoBean.java  |
| https://9cl.yangguanging.com/head/img/12971972/2021-12-20/e3dec7a4efa23a873441751e9477a7e9511798f8-5\  | com/avnight/x/o/p.java  |
| https://9ynefxy-1.sbs  | com/avnight/o/n7.java  |
| http://pv.sohu.com/cityjson?ie=utf-8  | com/avnight/tools/z.java  |
| http://qlaops.nongchang168.com/black  | com/avnight/tools/r/b.java  |
| http://qlaops.nongchang168.com/black  | com/avnight/tools/Base64ImageLoadUtil/d.java  |
| https://www.google.com/  | com/avnight/l/m7.java  |
| https://api.api98.xyz  | com/avnight/webservice/AvNightWebService.java  |
| https://dev-avnight-cpi.appdev.icu/API/  | com/avnight/webservice/AvNightWebService.java  |
| https://github.com/danikula/AndroidVideoCache/issues/88.  | com/danikula/videocache/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues/43.  | com/danikula/videocache/i.java  |
| https://github.com/danikula  | com/danikula/videocache/i.java  |
| https://github.com/danikula/AndroidVideoCache/issues.  | com/danikula/videocache/i.java  |
| http://%s:%d/%s  | com/danikula/videocache/k.java  |
| https://github.com/danikula/AndroidVideoCache/issues/134.  | com/danikula/videocache/k.java  |
| http://%s:%d/%s  | com/danikula/videocache/g.java  |
| https://www.google.com/speedtest/  | com/ngs/myngsspeedtest/e.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | d/g/a/a.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | g/a/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| http://schemas.xmlsoap.org/soap/envelope/  | org/fourthline/cling/transport/c/p.java  |
| http://schemas.xmlsoap.org/soap/encoding/  | org/fourthline/cling/transport/c/p.java  |
| http://www.sec.co.kr/dlna  | org/fourthline/cling/binding/xml/g.java  |
| https://app-av9-8631e.firebaseio.com  | 摸瓜V1引擎  |
| https://d1vcfwitp2um8b.cloudfront.net/api/host\_and.jsonb  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/encoding/  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/wsdl/soap/http?mtom=true  | 摸瓜V3引擎  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | 摸瓜V3引擎  |
| http://pv.sohu.com/cityjson?ie=utf-8  | 摸瓜V3引擎  |
| firebase-settings.crashlytics.com  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://9ynefxy-1.sbs  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/javaee  | 摸瓜V3引擎  |
| https://github.com/ReactiveX/RxJava/wiki/What  | 摸瓜V3引擎  |
| https://a9-cos.dango33.com/host\_and.jsonb  | 摸瓜V3引擎  |
| https://i.imgur.com/TOo1GxX.jpeg  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://av9av9-1318371851.cos.ap-guangzhou.myqcloud.com/host\_and.jsonb  | 摸瓜V3引擎  |
| https://9cl.yangguanging.com/head/img/12971972/2021-12-20/e3dec7a4efa23a873441751e9477a7e9511798f8-5  | 摸瓜V3引擎  |
| https://aomedia.org/emsg/ID3  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/javaee/javaee\_web\_services\_1\_2.xsd  | 摸瓜V3引擎  |
| https://av9av9-1309454273.cos.ap-guangzhou.myqcloud.com/host\_and.jsonb  | 摸瓜V3引擎  |
| https://openinstall.iavnight.com/api/  | 摸瓜V3引擎  |
| https://dev-avnight-cpi.appdev.icu/API/  | 摸瓜V3引擎  |
| http://qlaops.nongchang168.com/black  | 摸瓜V3引擎  |
| http://schemas.android.com/tools  | 摸瓜V3引擎  |
| https://app-av9-8631e.firebaseio.com  | 摸瓜V3引擎  |
| https://www.mzitu.com/  | 摸瓜V3引擎  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/jaxb  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/soap/envelope/  | 摸瓜V3引擎  |
| https://default.url  | 摸瓜V3引擎  |
| http://java.sun.com/xml/ns/jaxb/xjc  | 摸瓜V3引擎  |
| http://goo.gl/8Rd3yj  | 摸瓜V3引擎  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | 摸瓜V3引擎  |
| https://glassfish.dev.java.net/public/CDDL  | 摸瓜V3引擎  |
| https://av9av9-1318371851.cos.accelerate.myqcloud.com/host\_and.jsonb  | 摸瓜V3引擎  |
| http://dashif.org/guidelines/trickmode  | 摸瓜V3引擎  |
| http://goo.gl/naFqQk  | 摸瓜V3引擎  |
| www.google-analytics.com  | 摸瓜V3引擎  |
| http://schemas.xmlsoap.org/wsdl/soap/http  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| this@addfavdialog.childfragm  | com/avnight/o/r5.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | e/c/b/a/a.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.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: O=AvNight, OU=IT, CN=Eric Lin 签名算法: rsassa\_pkcs1v15 有效期自: 2016-05-06 02:54:23+00:00 有效期至: 2041-04-30 02:54:23+00:00 发行人: O=AvNight, OU=IT, CN=Eric Lin 序列号: 0x633954be 哈希算法: sha256 md5值: ae49c75d9549826f5b7adfb259649fcb sha1值: 7302bcc88f1adb1b280497f8b83627f720c59474 sha256值: 4d16c34c491c9e6ca60524f7c139f74127d9cc8b70258380a40f274ea562ea78 sha512值: 15d82146fc34a20ef65ef43518807548f188cf55defe2932f0e684cc74abd258098c7008f923ff548fb1da2f6f529b1317982d3fcf4b6828c2444527f828b811 公钥算法: rsa 密钥长度: 2048 指纹: f8128e85d6b21bfbdbbcb784f3d7be801f82df0129d340ff82e93a317cbed2ea**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "firebase\_database\_url" : "https://app-av9-8631e.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyCl9rvV7COaM\_j81LZPG7S9a\_zVp\_cXcj0"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyCl9rvV7COaM\_j81LZPG7S9a\_zVp\_cXcj0"  |
| "mixpanel\_token" : "266b05c861f7ff6d29c32e714bbf4794"  |
| "mixpanel\_token" : "266b05c861f7ff6d29c32e714bbf4794"  |
| "mixpanel\_token" : "266b05c861f7ff6d29c32e714bbf4794"  |

## **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.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\_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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 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.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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收  | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.avnight.Activity.LandingActivity.LandingActivity | **Schemes**: avnight://, http://, https://, **Hosts:** api2.i9999.pw, api2-devel.i999.pw,  |

**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。**