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

**黄瓜视频（ 8.62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 | 黄瓜视频 |
| 版本 | 8.62 |
| 包名 | ufdca.piwt.pfxpxa.oiee |
| 域名线索 | 12条 |
| URL线索 | 40条 |
| APP图标 |  |
| 分析日期 | 2025年6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 | xlav\_app\_20250611\_fpfs.apk |
| 文件大小 | 20.54MB |
| MD5值 | 7320bfa22cecab3f9c95081c10d293eb |
| SHA1值 | beaf3a3a67f6bd10c7e5b093a673daf8a7304182 |
| SHA256值 | f3eb818aa0cf14f87f55c12789c100faf8ced380fe43b057985da3fb2613dce7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 黄瓜视频 |
| 包名 | ufdca.piwt.pfxpxa.oiee |
| 主活动Activity | com.paulkman.nova.MainActivity |
| 安卓版本名称 | 8.62 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.android.com | IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.nova-traffic-1688.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| exoplayer.dev | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| logback.qos.ch | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| bense.tv | 没有服务器地理信息.  |
| ns.adobe.com | 没有服务器地理信息.  |
| api.ipify.org | IP: 104.26.12.205 所属国家: United States of America 地区: California 城市: San Francisco  |
| issuetracker.google.com | IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/google/gson/blob/main/Troubleshooting.md  | a7/a.java  |
| https://app.nova-traffic-1688.com  | b9/q.java  |
| http://www.slf4j.org/codes.html  | ch/qos/logback/classic/turbo/DynamicThresholdFilter.java  |
| http://www.slf4j.org/codes.html  | ch/qos/logback/classic/turbo/MDCFilter.java  |
| http://logback.qos.ch/css/classic.css  | ch/qos/logback/classic/html/UrlCssBuilder.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/classic/net/SocketReceiver.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/CoreConstants.java  |
| http://logback.qos.ch/manual/  | ch/qos/logback/core/CoreConstants.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/FileAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/OutputStreamAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/joran/action/AppenderRefAction.java  |
| http://xml.org/sax/features/validation  | ch/qos/logback/core/joran/event/SaxEventRecorder.java  |
| http://xml.org/sax/features/namespaces  | ch/qos/logback/core/joran/event/SaxEventRecorder.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/AbstractSocketAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/SyslogAppenderBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/net/SMTPAppenderBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/pattern/parser/Parser.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java  |
| http://logback.qos.ch/manual/appenders.html  | ch/qos/logback/core/rolling/SizeAndTimeBasedFNATP.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/TimeBasedFileNamingAndTriggeringPolicyBase.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/RollingFileAppender.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/rolling/helper/RenameUtil.java  |
| http://logback.qos.ch/codes.html  | ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | d4/h0.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | h1/g.java  |
| https://issuetracker.google.com/issues/new?component=413106  | o1/b2.java  |
| https://developer.android.com/training/articles/direct-boot  | o2/b.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | p5/a0.java  |
| https://app.nova-traffic-1688.com  | t8/h0.java  |
| https://app.nova-traffic-1688.com  | t8/m2.java  |
| https://api.ipify.org  | t8/c1.java  |
| https://app.nova-traffic-1688.com  | n2/f.java  |
| https://www.slf4j.org/codes.html  | qi/e.java  |
| https://app.nova-traffic-1688.com  | ha/h.java  |
| https://issuetracker.google.com/issues/new?component=907884&template=1466542  | ra/v2.java  |
| https://app.nova-traffic-1688.com  | gd/d.java  |
| https://github.com/google/gson/blob/main/Troubleshooting.md  | y6/c.java  |
| https://bense.tv  | 摸瓜V1引擎  |
| http://%s  | lib/arm64-v8a/libcf-msc.so  |
| http://%s  | lib/armeabi-v7a/libcf-msc.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/arm64-v8a/libcf-msc.so  |
| ftp@example.com  | lib/armeabi-v7a/libcf-msc.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15778476000  | nh/f.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, O=Sun, OU=JavaSoft, CN=Mark Jones 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-10 23:44:44+00:00 有效期至: 2080-03-13 23:44:44+00:00 发行人: C=US, O=Sun, OU=JavaSoft, CN=Mark Jones 序列号: 0xd92b455a78e80fbe 哈希算法: sha256 md5值: 221cc456305279f4ef261767006bcb95 sha1值: fe0539944e65ada98510d0de9344727ba38d41c4 sha256值: 4202fa5224cb002fc915bb5ec7e3a995be913dac1b056ce0afd15eb856069dab sha512值: d8667ba43c56a560da869c6ae4caaf591f6aa9448f4c97046315824a13bf9658517a43f14b028ddc79a3e5a6a810af8d0d5e7592c7b759e16afa2a51edb9b3e4 公钥算法: rsa 密钥长度: 2048 指纹: 328475a3562791ef2feee2213cc0b14f94847bcdbf9a4357b29f37f6a8ebee1d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "nova\_app\_auth\_button\_get\_phone\_number\_verify\_code" : "獲取驗證碼"  |
| "nova\_app\_auth\_button\_get\_phone\_number\_verify\_code\_retry\_count\_down" : "%1$d秒後重試"  |
| "nova\_app\_auth\_button\_sign\_up" : "立即註冊"  |
| "nova\_app\_auth\_dialog\_qrcode\_success" : "歡迎回來"  |
| "nova\_app\_auth\_mywallet" : "我的錢包"  |
| "nova\_app\_auth\_mywallet\_recharge" : "去充值"  |
| "nova\_app\_auth\_sign\_up\_successfully" : "註冊成功"  |
| "nova\_app\_auth\_vip" : "會員VIP"  |
| "nova\_app\_auth\_vip\_register" : "去開通"  |
| "nova\_app\_button\_my\_purchase\_api" : "我的購買(待接API)"  |
| "nova\_app\_button\_user" : "用戶:"  |
| "nova\_app\_debug\_enter\_password" : "請輸入密碼"  |
| "nova\_app\_setting\_account\_credentials" : "帳號憑證"  |
| "nova\_app\_auth\_button\_get\_phone\_number\_verify\_code" : "獲取驗證碼"  |
| "nova\_app\_auth\_button\_get\_phone\_number\_verify\_code\_retry\_count\_down" : "%1$d秒後重試"  |
| "nova\_app\_auth\_button\_sign\_up" : "立即註冊"  |
| "nova\_app\_auth\_dialog\_qrcode\_success" : "歡迎回來"  |
| "nova\_app\_auth\_mywallet" : "我的錢包"  |
| "nova\_app\_auth\_mywallet\_recharge" : "去充值"  |
| "nova\_app\_auth\_sign\_up\_successfully" : "註冊成功"  |
| "nova\_app\_auth\_vip" : "會員VIP"  |
| "nova\_app\_auth\_vip\_register" : "去開通"  |
| "nova\_app\_button\_my\_purchase\_api" : "我的購買(待接API)"  |
| "nova\_app\_button\_user" : "用戶:"  |
| "nova\_app\_debug\_enter\_password" : "請輸入密碼"  |
| "nova\_app\_setting\_account\_credentials" : "帳號憑證"  |

## **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.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.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.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。 |
| com.google.android.gms.permission.AD\_ID | 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| xjc.cmta.rpny.clojg.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 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。**