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

**君盛（ 9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 | 君盛 |
| 版本 | 9 |
| 包名 | vxxt.hxexg.eppkoispua.ecxmgfzryi |
| 域名线索 | 13条 |
| URL线索 | 1条 |
| APP图标 |  |
| 分析日期 | 2025年7月6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 | base.apk |
| 文件大小 | 3.2MB |
| MD5值 | b5e4355f796363492acd25607bab2d3c |
| SHA1值 | c95e0f41da29c954641c4fa63c09441fece54ee9 |
| SHA256值 | a1c6f10cd39a66faeb3eb591a86d8dd65145ff3b3e48607b69bca6887d89f22d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 君盛 |
| 包名 | vxxt.hxexg.eppkoispua.ecxmgfzryi |
| 主活动Activity | com.k70369.webviewtest.SplashActivity |
| 安卓版本名称 | 9 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| cn-hongkong.log.aliyuncs.com | IP: 47.244.67.194 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tbs.imtt.qq.com | IP: 211.97.84.73 所属国家: China 地区: Beijing 城市: Beijing  |
| youtrack.jetbrains.com | IP: 63.33.88.220 所属国家: Ireland 地区: Dublin 城市: Dublin  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| goo.gle | IP: 67.199.248.12 所属国家: United States of America 地区: New York 城市: New York City  |
| gitee.com | IP: 180.76.199.13 所属国家: China 地区: Beijing 城市: Beijing  |
| android.googlesource.com | IP: 108.177.98.82 所属国家: United States of America 地区: California 城市: Mountain View  |
| pms.mb.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.bilibili.com | IP: 218.60.18.18 所属国家: China 地区: Liaoning 城市: Fuxin  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://debugtbs.qq.com?10000  | 摸瓜V3引擎  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | 摸瓜V3引擎  |
| https://www.bilibili.com/video/BV1qmrfYgEDE  | 摸瓜V3引擎  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=:https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079/h  | 摸瓜V3引擎  |
| https://cn-hongkong.log.aliyuncs.com  | 摸瓜V3引擎  |
| https://pms.mb.qq.com/rsp2041https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | 摸瓜V3引擎  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | 摸瓜V3引擎  |
| https://gitee.com/wangjingdi88767  | 摸瓜V3引擎  |
| https://debugx5.qq.com  | 摸瓜V3引擎  |
| https://pms.mb.qq.com/rsp204  | 摸瓜V3引擎  |
| https://youtrack.jetbrains.com/issue/KT-55980  | 摸瓜V3引擎  |
| https://gitee.com/annabelle74100  | 摸瓜V3引擎  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | 摸瓜V3引擎  |
| https://gitee.com/wangjingdi88767#https://log.tbs.qq.com/ajax?c=dl&k=$https://log.tbs.qq.com/ajax?c=  | 摸瓜V3引擎  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | 摸瓜V3引擎  |
| https://www.bilibili.com/video/BV1RbUGYHE8u  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://android.googlesource.com/toolchain/llvm-project  | 摸瓜V3引擎  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://debugtbs.qq.com  | 摸瓜V3引擎  |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs  | 摸瓜V3引擎  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | 摸瓜V3引擎  |
| https://youtrack.jetbrains.com/issue/KT-46465  | 摸瓜V3引擎  |
| https://goo.gle/compose-feedback  | 摸瓜V3引擎  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

### **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: True 找到 1 个唯一证书 主题: C=(������������������������������), ST=(������������������), L=(���������������������), O=(������������), OU=(������������������), CN=(���������������) 签名算法: rsassa\_pkcs1v15 有效期自: 2025-02-27 12:20:20+00:00 有效期至: 2026-02-27 12:20:20+00:00 发行人: C=(������������������������������), ST=(������������������), L=(���������������������), O=(������������), OU=(������������������), CN=(���������������) 序列号: 0x7cbd266d 哈希算法: sha256 md5值: 3b31896b63dc3ff0c04946b6fc8b41f7 sha1值: 4410463839728253c6202b367f2aa1de305da0e8 sha256值: f9e48423bd0e896f3f12a2c7a30e89ef29a8186c401a64d621c7245406179038 sha512值: 758c3dbcdda328a4de0564e3b9c00cbad7a9f9d4c91ce51c3f523a358445cf7a818db1a16f603d586d41a604912b70dda5871964c1e0db9caaecdf3daa2c3732 公钥算法: rsa 密钥长度: 1024 指纹: 64795d5430dba73fb41c6e84656929c81043f498b080c011c9431667ebdf5be3**

## **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.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.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.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.WRITE\_SECURE\_SETTINGS | 系统需要 | 修改安全系统设置 | 允许应用程序修改系统固定好设置数据。不供普通应用程序使用 |
| 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 |
| vxxt.hxexg.eppkoispua.ecxmgfzryi.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |

## **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。**