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

**玖鼎e投（ 3.0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 | 玖鼎e投 |
| 版本 | 3.0 |
| 包名 | com.iv.phoneclient.nd.rel |
| 域名线索 | 19条 |
| URL线索 | 12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 | PhoneClient-H88Rel-3.0-1602.apk |
| 文件大小 | 77.75MB |
| MD5值 | 8b7a0e1ee00647c742c6c5ae867c1758 |
| SHA1值 | c269d30cc56c89ef1addd586b15f7bb95dfb3473 |
| SHA256值 | 90a24dd07ff67a4d63c1d9fd104b76f965f952d9fa2b6ffc4bc4e2c272b198d3 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 玖鼎e投 |
| 包名 | com.iv.phoneclient.nd.rel |
| 主活动Activity | com.iv.phoneclient.ui.SplashActivity |
| 安卓版本名称 | 3.0 |
| 安卓版本 | 1602 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| dt-central-api-http-l5.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| pagead2.googlesyndication.com | IP: 114.250.64.38 所属国家: China 地区: Beijing 城市: Beijing  |
| dt-central-api-http-l4.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dt-central-api.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dt-version-api.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.solaireresort.com | IP: 172.67.30.235 所属国家: United States of America 地区: California 城市: San Francisco  |
| newcoasthotels.com | IP: 45.76.153.24 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| schemas.android.com | 没有服务器地理信息.  |
| example.com | IP: 96.7.128.198 所属国家: United States of America 地区: California 城市: El Segundo  |
| www.midashotelandcasino.com | IP: 54.221.202.12 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| www.cityofdreamsmanila.com | IP: 18.155.68.121 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| app.hh-infra.com | 没有服务器地理信息.  |
| dt-central-api-http.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dt-cash-api.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dt-central-api-http-l3.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dt-auth-api.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.okadamanila.com | IP: 104.18.19.191 所属国家: United States of America 地区: California 城市: San Francisco  |
| dt-central-api-http-l2.star-link-rel.cc | IP: 18.163.114.61 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://dt-central-api.star-link-rel.cc)  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-central-api-http.star-link-rel.cc,  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-central-api-http-l2.star-link-rel.cc,  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-central-api-http-l3.star-link-rel.cc,  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-central-api-http-l4.star-link-rel.cc,  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-central-api-http-l5.star-link-rel.cc)  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-auth-api.star-link-rel.cc)  | com/iv/telebetcore/TelebetCore.java  |
| https://dt-cash-api.star-link-rel.cc)  | com/iv/telebetcore/TelebetCore.java  |
| http://example.com  | com/iv/telebetcore/manager/HttpManager$apiService$2.java  |
| https://app.hh-infra.com  | com/iv/telebetcore/utils/s.java  |
| https://dt-central-api-http.star-link-rel.cc,  | com/iv/telebetcore/central/CentralHttp.java  |
| https://dt-central-api-http-l2.star-link-rel.cc,  | com/iv/telebetcore/central/CentralHttp.java  |
| https://dt-central-api-http-l3.star-link-rel.cc,  | com/iv/telebetcore/central/CentralHttp.java  |
| https://dt-central-api-http-l4.star-link-rel.cc,  | com/iv/telebetcore/central/CentralHttp.java  |
| https://dt-central-api-http-l5.star-link-rel.cc  | com/iv/telebetcore/central/CentralHttp.java  |
| https://dt-central-api.star-link-rel.cc)  | com/iv/telebetcore/central/o.java  |
| https://dt-central-api.star-link-rel.cc  | com/iv/telebetcore/central/o.java  |
| https://dt-cash-api.star-link-rel.cc/api/v1/customer/auth\_app\_game  | com/iv/telebetcore/socket/BaseSocket.java  |
| https://dt-auth-api.star-link-rel.cc/api/v1/auth/app  | com/iv/telebetcore/socket/BaseSocket.java  |
| https://dt-version-api.star-link-rel.cc/api/game/config)  | com/iv/phoneclient/MainApplication.java  |
| https://dt-version-api.star-link-rel.cc/api/game/config?product\_id=H88&version=  | com/iv/phoneclient/task/a.java  |
| http://schemas.android.com/apk/res/android  | e4/c.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | e1/b.java  |
| https://www.cityofdreamsmanila.com/  | 摸瓜V1引擎  |
| https://www.midashotelandcasino.com/  | 摸瓜V1引擎  |
| https://newcoasthotels.com/  | 摸瓜V1引擎  |
| http://www.okadamanila.com/  | 摸瓜V1引擎  |
| https://www.solaireresort.com/  | 摸瓜V1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: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=TW, ST=Taipei, L=Taipei, OU=AG, CN=Ken Yang 签名算法: rsassa\_pkcs1v15 有效期自: 2016-08-14 10:48:06+00:00 有效期至: 3015-12-16 10:48:06+00:00 发行人: C=TW, ST=Taipei, L=Taipei, OU=AG, CN=Ken Yang 序列号: 0x57b04c66 哈希算法: sha1 md5值: 14a6231f48118f0e4f84e17354bbe490 sha1值: f8423ec983013f2121d9cbfb7744d47d33e81c9a sha256值: 22461b961a7c3a8666ad777e454d2bd7f9e65e5dbf586a3516a6bcfb994c9346 sha512值: 5f9b9d88287032680ae93acde851442f8872af5404abfc1720deea93b811bce40311937988e44674c771a60bb61262609a1008c72acdd5f1d19625212b28685b 公钥算法: rsa 密钥长度: 1024 指纹: 6b6e4aeb7ccdd15e92d3e7f7c46daeb3150891edff00214bb3d6ccc569dacfd9**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "5caf17f169584c05b64feb6c9ed2a1d1"  |
| "google\_api\_key" : "AIzaSyD6wuAphRPdDS7B1qjTJ28p-DjGuUBJxrc"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyD6wuAphRPdDS7B1qjTJ28p-DjGuUBJxrc"  |
| "notice\_password" : "密码需为8至12个字，至少包含一个英文大写、小写、数字。"  |
| "setting\_finger\_auth" : "指纹登入"  |
| "verify\_password" : "确认新密码"  |
| "notice\_password" : "The password must contain 8 to 12 characters, including at least one uppercase letter, lowercase letter, and digit."  |
| "setting\_finger\_auth" : "Log in by fingerprint"  |
| "verify\_password" : "Confirm New Password"  |
| "notice\_password" : "รหัสผ่านต้องมี 8–12 ตัวอักษร อย่างน้อยต้องมีหนึ่งตัวอักษรอังกฤษพิมพ์ใหญ่ พิมพ์เล็ก และตัวเลข."  |
| "setting\_finger\_auth" : "เข้าใช้งานโดยลายนิ้วมือ"  |
| "verify\_password" : "ยืนยันรหัสใหม่"  |
| "notice\_password" : "パスワードは8〜12字であること、また少なくとも１つ以上の英大文字と英小文字、数字を含んでいることが必要です。"  |
| "setting\_finger\_auth" : "指紋でログインする"  |
| "verify\_password" : "パスワード確認"  |
| "notice\_password" : "비밀번호는 8~12자, 영문 대문자, 소문자, 숫자 1개 이상이어야 합니다."  |
| "setting\_finger\_auth" : "지문 로그인"  |
| "verify\_password" : "새로운 패스워드 확인"  |

## **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\_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.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.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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.ACCESS\_ADSERVICES\_ATTRIBUTION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ADSERVICES\_AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| com.iv.phoneclient.nd.rel.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.iv.phoneclient.ui.SplashActivity | **Schemes**: coggame://, http://, https://, **Hosts:** com.iv.phoneclient.nd.rel,  |

**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。**