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

**戎耀今生（ 1.1.11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 | 戎耀今生 |
| 版本 | 1.1.11 |
| 包名 | com.inspur.vista.js |
| 域名线索 | 5条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年8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 | 戎耀今生.apk |
| 文件大小 | 100.44MB |
| MD5值 | 63b0762399dc01391a83e073a2c2e5ac |
| SHA1值 | ca3bdf4de69d3dc9e7569bf75b7317584ac8edc2 |
| SHA256值 | e0e09fa6b035ef243363456a503cf9b96d545a035d10d657b57a1805e6dbab90 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 戎耀今生 |
| 包名 | com.inspur.vista.js |
| 主活动Activity | com.inspur.vista.js.module.main.splash.SplashActivity |
| 安卓版本名称 | 1.1.11 |
| 安卓版本 | 22 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 121.10.217.171 | IP: 121.10.217.171 所属国家: China 地区: Guangdong 城市: Shantou  |
| 117.68.0.174 | IP: 117.68.0.174 所属国家: China 地区: Anhui 城市: Lu'an  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| gw.alipayobjects.com | IP: 116.136.165.43 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |
| https://gw.alipayobjects.com/os/bmw-prod/4444728e-bec0-4c86-bed3-37b25cb150bf.zip  | 摸瓜V2引擎  |
| https://gw.alipayobjects.com/os/bmw-prod/d14fca21-b2d8-4544-841a-fa4dd5c0a66c.zip  | 摸瓜V2引擎  |
| https://gw.alipayobjects.com/os/bmw-prod/d069028f-dd21-4455-a268-c5b8e0d8d895.zip  | 摸瓜V2引擎  |
| https://gw.alipayobjects.com/os/bmw-prod/5a6e95a9-46e8-454d-958e-d4d37a0521a1.dat  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010a4a4de3e3eb70993db.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010bda4de3e3eb70993e5.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010bfa4de3e3eb70993e7.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e01099a4de3e3eb70993d7.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61f23e7ca4de3e32d4da84bd.png  | 摸瓜V2引擎  |
| https://121.10.217.171:9002/\_ui/desktop/common/cmyy/image/app\_1.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010c0a4de3e3eb70993e9.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010b6a4de3e3eb70993e3.png  | 摸瓜V2引擎  |
| https://121.10.217.171:9002/\_ui/desktop/common/cmyy/image/app\_2.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010a2a4de3e3eb70993d9.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010afa4de3e3eb70993df.png  | 摸瓜V2引擎  |
| http://117.68.0.174:8001/tyjr-oss/tyjrfs/view/61e010ada4de3e3eb70993dd.png  | 摸瓜V2引擎  |
| https://121.10.217.171:9002/\_ui/desktop/common/cmyy/image/app\_4.png  | 摸瓜V2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: False 找到 1 个唯一证书 主题: C=1, ST=1, L=1, O=1, OU=1, CN=1 签名算法: rsassa\_pkcs1v15 有效期自: 2019-01-07 01:34:00+00:00 有效期至: 2044-01-01 01:34:00+00:00 发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1 序列号: 0x76805fad 哈希算法: sha256 md5值: d488748eefd5368d382ba1d1d95caeda sha1值: 8f49a9c5dc922ed33b21bbb536a35e2a2940ced1 sha256值: 3e3b481472c490965879c3628831599dba2d6e130a1a44a1b52340d4b06b60d4 sha512值: 1631234899df43b010d57e13c30ce055bc593c9f384ae6d34acda11d5a1887289b45fe3be6fddb1613efbcf627bd88174387eca81784de6eab30f250ce4689c1 公钥算法: rsa 密钥长度: 2048 指纹: 47a810a8879def88930e8b5e1cb1fd52836ab27ba9ea2a242eb169a2abc21245**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "agreement\_user" : "《齐鲁工惠用户协议》"  |
| "anonymous\_username" : "匿名用户"  |
| "check\_password" : "验证密码"  |
| "forget\_password" : "忘记密码"  |
| "laws\_and\_regulations" : "法律法规"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "mine\_identity\_authentication" : "网上统一可信安全身份认证（推荐）"  |
| "mine\_password" : "密码"  |
| "please\_input\_password" : "请输入6-16位密码"  |
| "please\_input\_pwd" : "请输入密码（最少6位）"  |
| "please\_set\_password" : "请设置密码"  |
| "please\_sure\_pwd" : "两次密码必须一致"  |
| "private\_ask" : "私密提问"  |
| "private\_question" : "私密"  |
| "reset\_password" : "重置密码"  |
| "sure\_pwd" : "确认密码"  |
| "agreement\_user" : "《齐鲁工惠用户协议》"  |
| "anonymous\_username" : "匿名用户"  |
| "check\_password" : "验证密码"  |
| "forget\_password" : "忘记密码"  |
| "laws\_and\_regulations" : "法律法规"  |
| "please\_input\_password" : "请输入6-16位密码"  |
| "please\_set\_password" : "请设置密码"  |
| "private\_ask" : "私密提问"  |
| "private\_question" : "私密"  |
| "reset\_password" : "重置密码"  |
| "agreement\_user" : "《齐鲁工惠用户协议》"  |
| "anonymous\_username" : "匿名用户"  |
| "check\_password" : "验证密码"  |
| "forget\_password" : "忘记密码"  |
| "laws\_and\_regulations" : "法律法规"  |
| "please\_input\_password" : "请输入6-16位密码"  |
| "please\_set\_password" : "请设置密码"  |
| "private\_ask" : "私密提问"  |
| "private\_question" : "私密"  |
| "reset\_password" : "重置密码"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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\_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.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.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.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\_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.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.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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。  |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| 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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.ACTIVITY\_RECOGNITION | 危险 | 允许应用程序识别身体活动 | 允许应用程序识别身体活动 |
| android.permission.BODY\_SENSORS | 危险 |  | 允许应用程序访问来自传感器的数据,用户使用这些数据来测量他/她体内发生的事情,例如心率 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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。**