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

**至尊（ 2.9.40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 | 至尊 |
| 版本 | 2.9.40 |
| 包名 | com.adamzeaug.apliencez |
| 域名线索 | 10条 |
| URL线索 | 21条 |
| APP图标 |  |
| 分析日期 | 2024年12月22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 | cp.apk |
| 文件大小 | 49.18MB |
| MD5值 | 44e0751b4844ca58c9edf1feb7b8ad2f |
| SHA1值 | b5f596c037c80280cf9f4c1fa36c2c44768ca698 |
| SHA256值 | 7ebcc0393c930a5adf35d0084369c697d48d0f4ee53096b5d3d5f76c458003f0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 至尊 |
| 包名 | com.adamzeaug.apliencez |
| 主活动Activity | org.zywx.wbpalmstar.uex11818.activity.SplashActivity |
| 安卓版本名称 | 2.9.40 |
| 安卓版本 | 59 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| tsis.jpush.cn | IP: 134.175.123.136 所属国家: China 地区: Beijing 城市: Beijing  |
| www.videolan.org | IP: 213.36.253.2 所属国家: France 地区: Ile-de-France 城市: Paris  |
| www.srket.com | 没有服务器地理信息.  |
| online.chat | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| m.huobi.com | IP: 104.244.43.6 所属国家: United States of America 地区: California 城市: San Francisco  |
| ce3e75d5.jpush.cn | IP: 120.233.50.37 所属国家: China 地区: Beijing 城市: Beijing  |
| office-test.jpushoa.com | IP: 172.17.5.42 所属国家: - 地区: - 城市: -  |
| 182.92.20.189 | IP: 182.92.20.189 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| bjuser.jpush.cn | IP: 122.9.9.237 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://zz.  | org/zywx/wbpalmstar/uex11818/webApi/HostApi.java  |
| https://download.  | org/zywx/wbpalmstar/uex11818/webApi/WebServerUrl.java  |
| https://online.chat  | org/zywx/wbpalmstar/uex11818/utils/r.java  |
| https://www.srket.com  | org/zywx/wbpalmstar/uex11818/utils/r.java  |
| https://m.huobi.com/  | org/zywx/wbpalmstar/uex11818/fragment/moneyPage/VcPayFragment.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | a/b/j.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | a/b/o.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | a/b/b.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | a/b/f.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | a/b/c/d.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | a/b/c/f.java  |
| https://tsis.jpush.cn  | cn/jiguang/ad/i.java  |
| https://bjuser.jpush.cn/v1/appawake/status  | cn/jiguang/aa/b.java  |
| http://182.92.20.189:9099/  | cn/jiguang/o/c.java  |
| https://ce3e75d5.jpush.cn/wi/cjc5tb  | cn/jiguang/analytics/android/a/c.java  |
| https://ce3e75d5.jpush.cn/bury/  | cn/jiguang/analytics/android/a/c.java  |
| http://office-test.jpushoa.com/sdk-config/wi/cjc5tb  | cn/jiguang/analytics/android/a/c.java  |
| http://office-test.jpushoa.com/bury-h5/  | cn/jiguang/analytics/android/a/c.java  |
| https://github.com/vinc3m1  | Mogua Engine V1  |
| https://github.com/vinc3m1/RoundedImageView  | Mogua Engine V1  |
| https://github.com/vinc3m1/RoundedImageView.git  | Mogua Engine V1  |
| http://www.videolan.org/x264.html  | lib/x86/libNodeMediaClient.so  |
| http://www.videolan.org/x264.html  | lib/arm64-v8a/libNodeMediaClient.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| this@cgpayfragment.context  | org/zywx/wbpalmstar/uex11818/fragment/moneyPage/f.java  |

### **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=PH, ST=Republika ng Pilipinas, L=Manila, O=Desheng Group, OU=App Team, CN=Bee Weng 签名算法: rsassa\_pkcs1v15 有效期自: 2020-04-16 08:55:33+00:00 有效期至: 2045-04-10 08:55:33+00:00 发行人: C=PH, ST=Republika ng Pilipinas, L=Manila, O=Desheng Group, OU=App Team, CN=Bee Weng 序列号: 0x77eafba5 哈希算法: sha256 md5值: d29773d08f8b4d848a6bb6588ad6ecbd sha1值: e0fd6dcc38e5706b503456db82da45e610981e22 sha256值: c95493843f28e94697a21496a77fdead1a272704dd64e96c53c671984ccf0e7d sha512值: 376183a630940cb22c87d157ba1308ea69fbdb970abc6a9cf86f3b8f3912a1735211bfc927f2ee03af708bab2639b44f646f1afc2de320d75924cd751a113ae3 公钥算法: rsa 密钥长度: 2048 指纹: de9b331316274b5b76f5c5a289a5d2373e54592d5240f20ea1855548e66d0285**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "icon\_user" : ""  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "updata\_pay\_pwd" : "修改提现密码成功，下次请使用新密码提现!"  |
| "updata\_user\_pwd" : "修改登录密码成功，下次请使用新密码登录!"  |
| "vip\_forget\_password" : "忘记帐号/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.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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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。 |
| com.adamzeaug.apliencez.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 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.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。 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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\_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.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\_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\_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.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.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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.zywx.wbpalmstar.uex11818.activity.SplashActivity | **Schemes**: ij3zx1://,  |

**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。**