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

**天泰电力（ 01.05.0076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 | 天泰电力 |
| 版本 | 01.05.0076 |
| 包名 | com.neusoft.eappesdl |
| 域名线索 | 18条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 63A284305B8B71E3FE6AF6A470B2128E.apk |
| 文件大小 | 18.57MB |
| MD5值 | 63a284305b8b71e3fe6af6a470b2128e |
| SHA1值 | 52dbc7834360b6a5ea2563357870107858cdd05c |
| SHA256值 | b339f87ce93b0404f0dbfc027912809fda284723aa1a516dcef434a5ee931f28 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 天泰电力 |
| 包名 | com.neusoft.eappesdl |
| 主活动Activity | org.zywx.wbpalmstar.engine.LoadingActivity |
| 安卓版本名称 | 01.05.0076 |
| 安卓版本 | 293 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mclient.alipay.com | IP: 116.142.245.227 所属国家: China 地区: Beijing 城市: Beijing  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| wgb.tx100.com | IP: 168.76.253.156 所属国家: South Africa 地区: Free State 城市: Bloemfontein  |
| api.weixin.qq.com | IP: 112.65.193.153 所属国家: China 地区: Shanghai 城市: Shanghai  |
| long.open.weixin.qq.com | IP: 112.65.193.150 所属国家: China 地区: Shanghai 城市: Shanghai  |
| open.appcan.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api.mch.weixin.qq.com | IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin  |
| wappaygw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |
| m.alipay.com | IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| open.weixin.qq.com | IP: 140.207.191.167 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mobilegw.alipaydev.com | IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| mobilegw.alipay.com | IP: 203.209.243.27 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| h5.m.taobao.com | IP: 221.194.162.215 所属国家: China 地区: Hebei 城市: Langfang  |
| discuz.3g2win.com | IP: 208.98.43.142 所属国家: United States of America 地区: Illinois 城市: Chicago  |
| paygate-yf.meituan.com | IP: 101.236.69.63 所属国家: China 地区: Beijing 城市: Beijing  |
| mcgw.alipay.com | IP: 116.142.245.206 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.aaa.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw-1-64.test.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.stable.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/sdk/cons/a.java  |
| https://mobilegw.alipaydev.com/mgw.htm  | com/alipay/sdk/cons/a.java  |
| http://m.alipay.com/?action=h5quit  | com/alipay/sdk/cons/a.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/cons/a.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/cons/a.java  |
| https://mcgw.alipay.com/sdklog.do  | com/alipay/sdk/packet/impl/c.java  |
| http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=$OrderId$&  | com/alipay/sdk/data/a.java  |
| https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple\  | com/alipay/test/a.java  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.java  |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s  | com/tencent/mm/opensdk/diffdev/a/d.java  |
| http://wgb.tx100.com/mobile/adver.wg  | org/zywx/wbpalmstar/engine/universalex/EUExWindow.java  |
| http://open.appcan.cn/myspace/delayInstallWidget.action  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/delayStartWidget.action  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/delayUnInstallWidget.action  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/getMyAppList.action?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/oauth2/getTxSessionKey.do?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/common/appcenter.html?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/oauth2/getLoginList.do?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/getAppList.action?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/installWidget.action?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/startWidget.action?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| http://open.appcan.cn/myspace/unInstallWidget.action?  | org/zywx/wbpalmstar/platform/myspace/CommonUtility.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?  | org/zywx/wbpalmstar/plugin/uexweixin/Constants.java  |
| https://api.weixin.qq.com/sns/auth?  | org/zywx/wbpalmstar/plugin/uexweixin/Constants.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?  | org/zywx/wbpalmstar/plugin/uexweixin/Constants.java  |
| https://api.weixin.qq.com/sns/userinfo?  | org/zywx/wbpalmstar/plugin/uexweixin/Constants.java  |
| https://api.weixin.qq.com/cgi-bin/token?grant\_type=client\_credential&appid=%s&secret=%s  | org/zywx/wbpalmstar/plugin/uexweixin/EuexWeChat.java  |
| https://api.weixin.qq.com/pay/genprepay?access\_token=%s  | org/zywx/wbpalmstar/plugin/uexweixin/EuexWeChat.java  |
| https://api.mch.weixin.qq.com/pay/unifiedorder  | org/zywx/wbpalmstar/plugin/uexweixin/utils/JsConst.java  |
| https://api.weixin.qq.com/sns/auth?access\_token=%s&openid=%s  | org/zywx/wbpalmstar/plugin/uexweixin/utils/JsConst.java  |
| https://api.weixin.qq.com/sns/oauth2/access\_token?appid=%s&secret=%s&code=%s&grant\_type=%s  | org/zywx/wbpalmstar/plugin/uexweixin/utils/JsConst.java  |
| https://api.weixin.qq.com/sns/oauth2/refresh\_token?appid=%s&grant\_type=%s&refresh\_token=%s  | org/zywx/wbpalmstar/plugin/uexweixin/utils/JsConst.java  |
| https://api.weixin.qq.com/sns/userinfo?access\_token=%s&openid=%s  | org/zywx/wbpalmstar/plugin/uexweixin/utils/JsConst.java  |
| http://wgb.tx100.com/mobile/wg-reg.wg  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://wgb.tx100.com/mobile/soft-reg.wg  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://wgb.tx100.com/mobile/soft-startup-report.wg  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://wgb.tx100.com/mobile/wg-reg.wg?ver=  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://wgb.tx100.com/mobile/soft-reg.wg?widgetOneId=  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://wgb.tx100.com/mobile/soft-startup-report.wg?widgetId=  | org/zywx/wbpalmstar/widgetone/dataservice/WHttpManager.java  |
| http://discuz.3g2win.com/source/plugin/zywx/rpc/widget\_upgrade.php  | org/zywx/wbpalmstar/widgetone/dataservice/WDataManager.java  |
| http://open.appcan.cn/oauth2/getLoginList.do?txSessionKey=  | org/zywx/wbpalmstar/widgetone/dataservice/WDataManager.java  |
| http://open.appcan.cn/common/appcenter.html?platFormId=1&pageindex=1  | org/zywx/wbpalmstar/widgetone/dataservice/WDataManager.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ml@rb.peyzb  | 摸瓜V2引擎  |
| xo@tq.dz  | 摸瓜V2引擎  |
| j@dl.hnj 5i@fy.3x  | 摸瓜V2引擎  |
| dti@tx.oz  | 摸瓜V2引擎  |
| -@g.yjj  | 摸瓜V2引擎  |
| e1fu@x.wz1 l@y7.68  | 摸瓜V2引擎  |
| v@z.0v yl@9.j9 pr@p.ǚz wc4@n-ӯ.gd ѫ@u.üiȵ aף@o.wjk y@5.jkyn ty@ኵ.pqsz rajwp8@xb.goվ  | 摸瓜V2引擎  |
| k@3x.ߣhy  | 摸瓜V2引擎  |
| 1@r6\_.mg k@dp.\_98h ڙ@o.qnt  | 摸瓜V2引擎  |
| sy@q.wi  | 摸瓜V2引擎  |
| 9@f.6mil  | 摸瓜V2引擎  |
| -f@u.uȕ  | 摸瓜V2引擎  |
| 㒢b0@l.桛fr  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=china, ST=liaoning, L=dalian, O=neusoft, OU=neusoft, CN=neusoft 签名算法: rsassa\_pkcs1v15 有效期自: 2021-01-07 04:32:18+00:00 有效期至: 4758-12-05 04:32:18+00:00 发行人: C=china, ST=liaoning, L=dalian, O=neusoft, OU=neusoft, CN=neusoft 序列号: 0x4ef19893 哈希算法: sha256 md5值: b493396391de3cee051439352a9ca66a sha1值: 95a75b6bf904aeb0ec985110ae049f96bd06f534 sha256值: e79948aa0a06a3a23d98876cfd23cc170f347c68d6b0f84a71789f49228ec3f0 sha512值: d62cdd26a80e8108b5d2eec1a2a3cd2622219cf0dd551abbbaf5ed13b57c6bdbab3749eca6b7ce89d94848ff5724b35d7a0d34bcfbc7b0c7dc818da184058875**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "appkey" : "cd8acf1c-4dc3-a937-2631-fc50ac048819"  |
| "err\_auth\_denied" : "认证被否决"  |
| "plugin\_file\_type\_certificate" : "证书"  |
| "plugin\_file\_type\_certificate" : "Certificate"  |

## **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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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\_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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.neusoft.eappesdl.uexdevice.permission | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.zywx.wbpalmstar.engine.EBrowserActivity | **Schemes**: appcanaaajs10002://,  |

**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。**