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

**CoinW（ 9.6.8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 | CoinW |
| 版本 | 9.6.8 |
| 包名 | com.coinw.weba |
| 域名线索 | 63条 |
| URL线索 | 86条 |
| APP图标 |  |
| 分析日期 | 2024年11月20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 | coinw.apk |
| 文件大小 | 84.07MB |
| MD5值 | f5bc2662063c1ae48dea7223a2a188f9 |
| SHA1值 | b588e73c723cd85a159a74d2ea493ac1a47f32ee |
| SHA256值 | 4f724ce68541f3fccad9ab50d5780bd03fd3578ddeae4022b4e0fed2f41e6837 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | CoinW |
| 包名 | com.coinw.weba |
| 主活动Activity | mage.bywop.byw.ui.activity.StartUpActivity |
| 安卓版本名称 | 9.6.8 |
| 安卓版本 | 906080 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.umeng.com | IP: 59.82.31.160 所属国家: China 地区: Beijing 城市: Beijing  |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.248 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| futuresapi.ifuboug.cn | IP: 138.113.58.32 所属国家: United States of America 地区: California 城市: Monrovia  |
| developer.mozilla.org | IP: 13.225.183.17 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| btc602.oss-cn-shenzhen.aliyuncs.com | IP: 120.77.167.204 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.coinw.academy | IP: 208.43.237.140 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| appn.ifuboug.cn | IP: 138.113.58.32 所属国家: United States of America 地区: California 城市: Monrovia  |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息.  |
| developer.android.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| check-ipv4.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| logs.browser-intake-datadoghq.com | IP: 3.233.152.248 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| wannos.127.net | IP: 223.252.196.43 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| alogsus.umeng.com | IP: 223.109.148.177 所属国家: China 地区: Beijing 城市: Beijing  |
| statistic.live.126.net | IP: 183.131.177.121 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.baidu.com | IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding  |
| image.cnamedomain.com | 没有服务器地理信息.  |
| nosup-hz1.127.net | IP: 45.127.129.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.hyperpay.tech | IP: 170.33.13.190 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| plus.google.com | IP: 69.63.176.143 所属国家: United States of America 地区: California 城市: Menlo Park  |
| mum.alibabachengdun.com | IP: 203.119.169.27 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.cs.caltech.edu | IP: 131.215.140.31 所属国家: United States of America 地区: California 城市: Pasadena  |
| lbs-test.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| schemas.xmlsoap.org | IP: 13.107.238.49 所属国家: United States of America 地区: Washington 城市: Redmond  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| cro-dualstack.cn-hangzhou.aliyuncs.com | IP: 47.111.202.72 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pre-verify-cloud.alibaba-inc.com | IP: 59.82.29.53 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| oss.aliyuncs.com | IP: 118.178.29.5 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlog.umeng.com | IP: 223.109.148.143 所属国家: China 地区: Beijing 城市: Beijing  |
| pest.w3.org | 没有服务器地理信息.  |
| lbs.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| cdn-mum.alibabachengdun.com | IP: 42.81.21.187 所属国家: China 地区: Tianjin 城市: Tianjin  |
| rum.browser-intake-datadoghq.com | IP: 3.233.153.142 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| btc602.oss-accelerate.aliyuncs.com | IP: 8.131.131.12 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ping.microblink.com | IP: 104.22.79.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| check.fratrsese.com | IP: 138.113.58.32 所属国家: United States of America 地区: California 城市: Monrovia  |
| exoplayer.dev | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| aaid.umeng.com | IP: 218.91.197.67 所属国家: China 地区: Jiangsu 城市: Nantong  |
| check-ipv6.netease.im | 没有服务器地理信息.  |
| baltazar.microblink.com | IP: 104.22.79.119 所属国家: United States of America 地区: California 城市: San Francisco  |
| app.mi.com | IP: 183.84.5.210 所属国家: China 地区: Beijing 城市: Beijing  |
| coinw.udesk.cn | IP: 203.107.54.59 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dr.netease.im | IP: 183.131.177.88 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ulogs.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| t.me | IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Lowestoft  |
| api.megvii.com | IP: 123.57.112.143 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| market.m.taobao.com | IP: 111.225.210.166 所属国家: China 地区: Hebei 城市: Langfang  |
| coinw.zendesk.com | IP: 104.18.249.37 所属国家: United States of America 地区: California 城市: San Francisco  |
| imtest.netease.im | IP: 59.111.209.232 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| schemas.microsoft.com | IP: 13.107.238.49 所属国家: United States of America 地区: Washington 城市: Redmond  |
| ns.adobe.com | 没有服务器地理信息.  |
| pslog.umeng.com | IP: 59.82.31.95 所属国家: China 地区: Beijing 城市: Beijing  |
| 118.184.178.238 | IP: 118.184.178.238 所属国家: China 地区: Jiangsu 城市: Changzhou  |
| hyperpay.tech | IP: 170.33.13.190 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| plbslog.umeng.com | IP: 36.156.202.68 所属国家: China 地区: Beijing 城市: Beijing  |
| trace.browser-intake-datadoghq.com | IP: 3.233.147.191 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| ulogs.umengcloud.com | IP: 223.109.148.141 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.cs.caltech.edu/  | org/json/Test.java  |
| http://pest.w3.org/'/><bCard  | org/json/Test.java  |
| http://schemas.xmlsoap.org/soap/envelope/\  | org/json/Test.java  |
| http://www.w3.org/1999/XMLSchema-instance\  | org/json/Test.java  |
| http://www.w3.org/1999/XMLSchema\  | org/json/Test.java  |
| http://schemas.xmlsoap.org/soap/encoding/\  | org/json/Test.java  |
| https://(?:(?:(?:(?:nv  | jumio/core/e.java  |
| https://check.fratrsese.com/  | ˉ/ﾞﾞ/ʻ/ˆ/C13334.java  |
| https://appn.ifuboug.cn  | ˉ/ﾞﾞ/ʻ/ʽ/C13112.java  |
| https://github.com/iProov/android  | ˉ/ᵢ/ʻ/ˋ/C12917.java  |
| https://logs.browser-intake-datadoghq.com  | ˉ/י/ʻ/ʽ/ʻ/C8378.java  |
| https://trace.browser-intake-datadoghq.com  | ˉ/י/ʻ/ʽ/ʻ/C8378.java  |
| https://rum.browser-intake-datadoghq.com  | ˉ/י/ʻ/ʽ/ʻ/C8378.java  |
| https://plus.google.com/  | ˉ/ᵎ/ʻ/ʾ/ʼ/ˊ/C10512.java  |
| https://developer.android.com/reference/com/google/android/play/core/install/model/InstallErrorCode  | ˉ/ᵎ/ʻ/ˆ/ʻ/ʾ/C11674.java  |
| https://developer.android.com/reference/com/google/android/play/core/splitinstall/model/SplitInstallErrorCode.html  | ˉ/ᵎ/ʻ/ˆ/ʻ/ˋ/C11781.java  |
| http://schemas.android.com/apk/res/android  | ˉ/ᵎ/ʻ/ˆ/ʻ/ʿ/C11741.java  |
| https://developer.android.com/reference/com/google/android/play/core/assetpacks/model/AssetPackErrorCode.html  | ˉ/ᵎ/ʻ/ˆ/ʻ/ʼ/C11542.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | ˉ/ᵎ/ʻ/ʼ/C9261.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | ˉ/ᵎ/ʻ/ʼ/ʽי/C9538.java  |
| https://x</LA\_URL>  | ˉ/ᵎ/ʻ/ʼ/ʽי/C9552.java  |
| https://x  | ˉ/ᵎ/ʻ/ʼ/ʽי/C9552.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | ˉ/ᵎ/ʻ/ʼ/ʽⁱ/C10252.java  |
| http://www.w3.org/ns/ttml  | ˉ/ᵎ/ʻ/ʼ/ʽᵔ/ⁱ/C10129.java  |
| http://ns.adobe.com/xap/1.0/  | ˉ/ᵎ/ʻ/ʼ/ʽـ/ˉˉ/C9634.java  |
| http://dashif.org/guidelines/trickmode  | ˉ/ᵎ/ʻ/ʼ/ʽᵎ/ʻʼ/C9857.java  |
| http://dashif.org/guidelines/trickmode  | ˉ/ᵎ/ʻ/ʼ/ʽᵎ/ʻʼ/ˑ/C9873.java  |
| http://dashif.org/guidelines/last-segment-number  | ˉ/ᵎ/ʻ/ʼ/ʽᵎ/ʻʼ/ˑ/C9873.java  |
| https://appn.ifuboug.cn  | ˉ/ʼ/ʻ/ˈ/ˋ/View$OnClickListenerC6322.java  |
| https://www.coinw.academy/mobile/download.html  | ˉ/ʼ/ʻ/ˈ/ˋ/View$OnClickListenerC6325.java  |
| https://futuresapi.ifuboug.cn  | ˉ/ʼ/ʻ/ˈ/ˋ/View$OnClickListenerC6323.java  |
| https://www.coinw.academy/  | ˉ/ʼ/ʻ/ˈ/ˋ/View$OnClickListenerC6324.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/tr/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/pt/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/ru/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://coinw.zendesk.com/hc/en-us/articles/6764563347097  | ˉ/ʼ/ʻ/ˈ/ˋ/ˋ/View$OnClickListenerC6337.java  |
| https://btc602.oss-accelerate.aliyuncs.com/coinw2/domain.json  | ˉ/ʼ/ʻ/ˈ/ˋ/ˏ/C6357.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | ʼʼ/ˑ/ʻ/C5188.java  |
| https://futuresapi.ifuboug.cn  | mage/bywop/byw/ui/activity/StartUpActivity.java  |
| https://www.coinw.academy/  | mage/bywop/byw/ui/activity/StartUpActivity.java  |
| https://btc602.oss-cn-shenzhen.aliyuncs.com/coinw2/com-google-android-apps-authenticator2-5000100-51532195-7f40d893535070cde0ac091d7105bb66.apk  | mage/bywop/byw/ui/activity/bindgoogle/BindGoogleOneActivity.java  |
| http://app.mi.com/detail/163525?ref=search  | mage/bywop/byw/ui/activity/bindgoogle/BindGoogleOneActivity.java  |
| https://api.megvii.com/faceid/lite/do?token=  | mage/bywop/byw/ui/activity/renzheng/WebviewActivity.java  |
| https://coinw.udesk.cn/im\_client/?web\_plugin\_id=99712&group\_id=133212&language=zh-cn  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://coinw.udesk.cn/im\_client/?web\_plugin\_id=99722&group\_id=133042&language=en-us  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://coinw.udesk.cn/im\_client/?web\_plugin\_id=99732&group\_id=133202&language=ko  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://coinw.udesk.cn/im\_client/?web\_plugin\_id=101702&agent\_id=177452&group\_id=135472&language=vi  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://t.me/CoinwPT  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://coinw.zendesk.com/hc/en-us/requests/new  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://t.me/CoinwRU  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://t.me  | mage/bywop/byw/ui/fragment/maintab04/WebViewActivity.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/en-us/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/tr/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/pt/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://coinw.zendesk.com/hc/ru/articles/9820605408793  | mage/bywop/byw/ui/fragment/maintab04/GridWebViewActivity.java  |
| https://www.coinw.academy/mobile/download.html  | mage/bywop/reform/home/activity/ShareActivity.java  |
| https://www.coinw.academy/mobile/download.html  | mage/bywop/reform/home/activity/kline2/KLineActivity$showPop$2.java  |
| https://www.hyperpay.tech/?con=api&ctl=coinw\_banner  | mage/bywop/reform/mine/activity/MoneyManagerActivity.java  |
| https://www.hyperpay.tech/?con=api&ctl=coinw\_product&type=  | mage/bywop/reform/mine/fragment/MoneyManagerFragment.java  |
| https://www.hyperpay.tech/data/upload/  | ʻʾ/ʻ/ˈ/ˆ/ʼ/C3408.java  |
| https://www.hyperpay.tech/data/upload/  | ʻʾ/ʻ/ˈ/ˆ/ʼ/C3420.java  |
| https://www.hyperpay.tech/data/upload/  | ʻʾ/ʻ/ˈ/ˆ/ʼ/C3410.java  |
| https://www.hyperpay.tech/data/upload/  | ʻʾ/ʻ/ˈ/ˆ/ʼ/C3411.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/tr/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/pt/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/ru/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/en-us/articles/8434461474329  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3515.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/tr/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/pt/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/ru/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| https://coinw.zendesk.com/hc/en-us/articles/360052353313  | ʻʾ/ʻ/ˋ/ˎˎ/View$OnClickListenerC3500.java  |
| http://118.184.178.238  | ʻʾ/ʻ/ˋ/ˋˋ/C3482.java  |
| https://btc602.oss-accelerate.aliyuncs.com/coinw2/domain.json  | ʻʾ/ʻ/ˋ/ˋˋ/C3476.java  |
| https://appn.ifuboug.cn  | ʻʾ/ʻ/ˋ/ˋˋ/C3476.java  |
| https://futuresapi.ifuboug.cn  | ʻʾ/ʻ/ˋ/ˋˋ/C3476.java  |
| https://www.coinw.academy/  | ʻʾ/ʻ/ˋ/ˋˋ/C3476.java  |
| https://www.coinw.academy/mobile/download.html  | ʻʾ/ʻ/ˋ/ˋˋ/C3476.java  |
| https://www.coinw.academy/mobile/download.html  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᴵᴵ/C2966.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/tr/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/pt/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/ru/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/en-us/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ᵔ/C3003.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/pt-pt/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/tr-tr/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://coinw.zendesk.com/hc/en-us/articles/360033924414  | ʻʾ/ʻ/ʻ/ˆ/ʻ/ⁱ/C3049.java  |
| https://www.coinw.academy/  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://btc602.oss-cn-shenzhen.aliyuncs.com/app\_download\_test/5MB.zip  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://hyperpay.tech/app\_down?lang=zh-cn  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://hyperpay.tech/app\_down?lang=en-us  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://hyperpay.tech/app\_down?lang=ko-kr  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://hyperpay.tech/app\_down?lang=vi-vn  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://hyperpay.tech/app\_down?lang=zh-tw  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/en-us/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/tr/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/4404653630745  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/pt/articles/4404961645465  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ru/articles/4404961645465  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/en-us/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ko-kr/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/tr/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/pt/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ru/articles/8741829768473  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-cn  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/en-us  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ko-kr  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/vi-vn  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-tw  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/tr  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/pt  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ru  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/en-us/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/vi-vn/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/tr/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/zh-tw/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/pt/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| https://coinw.zendesk.com/hc/ru/articles/7682295586201  | ʻʾ/ʻ/ʻ/ʿ/C2788.java  |
| http://schemas.android.com/apk/res/android  | ʽʽ/ʻ/ʻ/ʻ/ˈ/C5649.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| https://developer.android.com/training/permissions/requesting.html  | com/jumio/sdk/exceptions/MissingPermissionException.java  |
| https://futuresapi.ifuboug.cn  | com/legend/modular\_contract\_sdk/component/net/RetrofitInstance$retrofitClient$2.java  |
| https://github.com/Justson/AgentWeb  | com/just/agentweb/BaseAgentWebFragment.java  |
| https://errlogos.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/d/a.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/d/a.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/a/i/c.java  |
| https://github.com/iProov/android/wiki/Frequently-Asked-Questions).  | com/iproov/sdk/ui/activity/Cdo.java  |
| https://mum.alibabachengdun.com/repTd.json?  | com/alibaba/wireless/security/framework/SGApmMonitorManager.java  |
| http://cdn-mum.alibabachengdun.com/sg7sX1/rYxU/pDDw/  | com/alibaba/wireless/security/framework/SGApmMonitorManager.java  |
| https://market.m.taobao.com/app/msd/m-rp-h5/cloud.html  | com/alibaba/security/realidentity/RPVerify.java  |
| http://oss-cn-hangzhou.aliyuncs.com  | com/alibaba/security/realidentity/build/ca.java  |
| https://market.m.taobao.com/app/msd/m-rp-h5/cloud.html  | com/alibaba/security/realidentity/build/j.java  |
| http://oss.aliyuncs.com  | com/alibaba/security/realidentity/build/dd.java  |
| http://127.0.0.1  | com/alibaba/security/realidentity/build/dd.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/security/realidentity/build/dd.java  |
| http://image.cnamedomain.com'!  | com/alibaba/security/realidentity/build/dd.java  |
| https://ip.  | com/alibaba/security/realidentity/build/bv.java  |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or  | com/alibaba/security/realidentity/build/bv.java  |
| http://image.cnamedomain.com'!  | com/alibaba/security/realidentity/build/bv.java  |
| https://cro-dualstack.cn-hangzhou.aliyuncs.com  | com/alibaba/security/realidentity/http/BaseHttpManager.java  |
| http://pre-verify-cloud.alibaba-inc.com  | com/alibaba/security/realidentity/http/BaseHttpManager.java  |
| http://statistic.live.126.net/statics/report/common/form  | com/netease/nimlib/d/f/a.java  |
| https://statistic.live.126.net/dispatcher/req  | com/netease/nimlib/c/b.java  |
| https://statistic.live.126.net/  | com/netease/nimlib/c/b/d/b.java  |
| http://wannos.127.net/lbs;http://wannos-hz.127.net/lbs;http://wannos-bj.127.net/lbs;http://wannos-oversea.127.net/lbs;http://223.252.196.38/lbs  | com/netease/nimlib/f/g.java  |
| https://nosup-hz1.127.net  | com/netease/nimlib/f/g.java  |
| https://lbs-test.netease.im/lbs/conf.jsp  | com/netease/nimlib/f/e.java  |
| https://imtest.netease.im/1.gif  | com/netease/nimlib/f/e.java  |
| http://check-ipv4.netease.im/  | com/netease/nimlib/f/e.java  |
| http://check-ipv6.netease.im/  | com/netease/nimlib/f/e.java  |
| https://imtest.netease.im/lbsrc/conf.jsp  | com/netease/nimlib/f/e.java  |
| https://lbs.netease.im/lbs/conf.jsp  | com/netease/nimlib/f/e.java  |
| https://dr.netease.im/1.gif  | com/netease/nimlib/f/e.java  |
| https://www.baidu.com/  | com/allenliu/versionchecklib/utils/UpgradeUtils.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| http://schemas.android.com/apk/res-auto  | com/microblink/blinkbarcode/view/CameraViewGroup.java  |
| https://baltazar.microblink.com/api/v1/status/check  | com/microblink/blinkbarcode/secured/IllllIIlII.java  |
| https://ping.microblink.com/api/v1/ping  | com/microblink/blinkbarcode/secured/IIllIlIlII.java  |
| https://coinw.zendesk.com/hc/zh-cn/articles/360047121113  | Mogua Engine V1  |
| https://coinw.zendesk.com/hc/en-us/articles/360047121113  | Mogua Engine V1  |
| https://coinw.zendesk.com/hc/ko-kr/articles/360047121113  | Mogua Engine V1  |
| http://',  | Mogua Engine V2  |
| https://';  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| khare@mci.net adam@cs.caltech  | org/json/Test.java  |
| u0013android@android.com0 u0013android@android.com  | ˉ/ᵎ/ʻ/ʾ/ʼ/BinderC10598.java  |
| 如需申请成为商户请发邮件到support@coinw.com 如需申请成为商家请发邮件到support@coinw.com support@coinw.com support@byw.ai support@coinw.com으로 如需申請成為商戶請發郵件到support@coinw.com 如需申請成為商家請發郵件到support@coinw.com  | Mogua Engine V1  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 16222222222  | ˉ/ᵎ/ʻ/ʼ/ʽـ/ˈˈ/C9625.java  |
| 17512775099  | ˉ/ᵎ/ʼ/ʽ/C12128.java  |
| 15102222222  | mage/bywop/byw/ui/fragment/maintab04/NetworkDetectActivity$doDetect$1.java  |
| 15112222222  | mage/bywop/byw/ui/fragment/maintab04/NetworkDetectActivity$doDetect$1.java  |
| 15552000000  | mage/bywop/reform/mine/activity/TradeOrderListActivity.java  |

## **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=cn, ST=bj, L=bj, O=cw, OU=cw, CN=coin 签名算法: rsassa\_pkcs1v15 有效期自: 2022-11-06 15:46:46+00:00 有效期至: 2047-10-31 15:46:46+00:00 发行人: C=cn, ST=bj, L=bj, O=cw, OU=cw, CN=coin 序列号: 0x422cf34d 哈希算法: sha256 md5值: bee9d182aa7b95e3f3e1914d9ec0f4c2 sha1值: f5f7e198a02ed983b72ee44f77259fbea371e4a7 sha256值: 76bf0a278ae70d4264bf7164adb59ba985efdefe8aa866b5c0e69b2809b03d2f sha512值: 21008cdfa9835f9c19c8a827835e309e3fffc8c089a568a1f5ed7795fbfc70b14ece4c48b2fe4631534e04717481d07628f88b1f828eaa8e708bfcc6cc58247b 公钥算法: rsa 密钥长度: 2048 指纹: 7cab462bde7e3c372ff7cd9cf835c73f5d193e64517ac70fb303946330150679**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "agree\_certificate" : "同意认证"  |
| "face\_auth\_announce" : "由阿里实人认证提供服务"  |
| "face\_detect\_auth\_begin\_cancel" : "放弃"  |
| "face\_detect\_auth\_begin\_ok" : "开始验证"  |
| "face\_detect\_auth\_begin\_title" : "安全验证"  |
| "face\_detect\_auth\_pass" : "验证通过"  |
| "face\_detect\_token\_expired\_or\_invalid" : "认证token无效或已过期"  |
| "face\_detect\_token\_repeate\_submit" : "认证已通过，重复提交。"  |
| "finish\_auth" : "1.一阶累计净划入%sUSDT可获得%sUSDT泥码 2.二阶累计净划入%sUSDT可获得%sUSDT泥码"  |
| "identity\_privacy\_authorization\_statement" : " 本APP运营方为确保用户身份真实性，向您提供更好的安全保障，您可以通过提交身份证等身份信息或面部特征等生物识别信息（均属个人敏感信息）来完成具体产品服务所需要或必要的实人认证。上述信息将使用与验证用户身份真实性。 我们会采用行业领先的技术来保护您提供的个人信息，并使用加密、限权等方式避免其被用于其他用途。 点击同意则表示本人同意我们根据以上方式和目的收集、使用及存储您提供的本人身份材料、面部特征等信息用于实人认证。"  |
| "identity\_privacy\_authorization\_statement\_title" : "授权声明"  |
| "iproov\_\_authenticate" : "Authenticate"  |
| "mc\_sdk\_one\_key\_close\_position" : "一键平仓"  |
| "no\_authentication" : "您尚未完成实名认证"  |
| "pwd\_rule" : "密码必须是8-32位，同时包含大小写字母和数字。登录密码不允许与交易密码一致"  |
| "pwd\_rule\_contain\_lower" : "密码必须包含小写字母"  |
| "pwd\_rule\_contain\_number" : "密码必须包含数字"  |
| "pwd\_rule\_contain\_upper" : "密码必须包含大写字母"  |
| "pwd\_rule\_length" : "密码必须是8-32位"  |
| "reject\_certificate" : "拒绝认证"  |
| "str\_pwd\_tip" : "8-32位；必须包含大小写英文、数字、特殊字符，其中至少2种。"  |
| "str\_pwd\_twice\_verify\_tip" : "两次密码不一致"  |
| "team\_authentication" : "身份验证"  |
| "team\_invitee\_authentication" : "被邀请人身份验证"  |
| "team\_invitee\_need\_authen" : "需要验证"  |
| "team\_invitee\_not\_need\_authen" : "不需要验证"  |
| "team\_need\_authentication" : "需要身份验证"  |
| "two\_pwd\_different" : "两次密码输入不一致！"  |
| "agree\_certificate" : "Xác thực đồng ý"  |
| "finish\_auth" : "1. Chuyển ròng tích lũy bậc một của%sUSDT có thể nhận được mã bùn%sUSDT n2. Chuyển thực tích lũy bậc hai của%sUSDT có thể nhận được mã bùn%sUSDT"  |
| "mc\_sdk\_one\_key\_close\_position" : "Đóng hết"  |
| "no\_authentication" : "Bạn chưa hoàn thành xác minh tên thật"  |
| "pwd\_rule\_contain\_lower" : "Mật khẩu phải chứa các chữ cái viết thường"  |
| "pwd\_rule\_contain\_number" : "Mật khẩu phải chứa số"  |
| "pwd\_rule\_contain\_upper" : "Mật khẩu phải có chữ in hoa"  |
| "pwd\_rule\_length" : "Mật khẩu phải có 8-32 chữ số"  |
| "reject\_certificate" : "Từ chối xác thực"  |
| "str\_pwd\_tip" : "8-32 ký tự.Yêu cầu chứa chữ tiếng Anh viết hoa và thường, chữ số, ký tự đặc biệt.Tối thiểu 2 loại trong số đó"  |
| "str\_pwd\_twice\_verify\_tip" : "Hai mật khẩu không khớp"  |
| "team\_authentication" : "Xác minh thân phận"  |
| "team\_invitee\_authentication" : "Xác thực mời người"  |
| "team\_invitee\_need\_authen" : "Cần xác minh"  |
| "team\_invitee\_not\_need\_authen" : "Không cần xác minh"  |
| "team\_need\_authentication" : "Yêu cầu xác thực thân phận"  |
| "two\_pwd\_different" : "Hai mục nhập mật khẩu không nhất quán!"  |
| "agree\_certificate" : "Agree"  |
| "finish\_auth" : "1.First-level cumulative net transfer reaching %sUSDT can get %sUSDT non-neg chip 2.Second-level cumulative net transfer reaching %sUSDT can get %sUSDT non-neg chip"  |
| "mc\_sdk\_one\_key\_close\_position" : "Liquidate"  |
| "no\_authentication" : "You haven't completed the identity verification"  |
| "pwd\_rule" : "The password must be 8-32 digits and contain both uppercase and lowercase letters and numbers. The login password cannot be the same as the trading password"  |
| "pwd\_rule\_contain\_lower" : "Password must contain lowercase letters"  |
| "pwd\_rule\_contain\_number" : "Password must contain numbers"  |
| "pwd\_rule\_contain\_upper" : "Password must contain uppercase letters"  |
| "pwd\_rule\_length" : "Password must be 8-32 digits"  |
| "reject\_certificate" : "Refuse"  |
| "str\_pwd\_tip" : "8-32 bits; must contain uppercase and lowercase English, numbers, special characters, at least 2 of them."  |
| "str\_pwd\_twice\_verify\_tip" : "Two passwords entered are inconsistent"  |
| "team\_authentication" : "Authentication"  |
| "team\_invitee\_authentication" : "Invitee authentication"  |
| "team\_invitee\_need\_authen" : "Authentication required"  |
| "team\_invitee\_not\_need\_authen" : "No authentication required"  |
| "team\_need\_authentication" : "Need authentication"  |
| "two\_pwd\_different" : "Two entered password must be consistent!"  |
| "agree\_certificate" : "동의"  |
| "finish\_auth" : "1.첫 번째 주문 누적 순 전송 %sUSDT는 %sUSDT 웰컴보너스 2를 얻을 수 있습니다. 두 번째 주문 누적 순 전송 %sUSDT 웰컴보너스 2를 얻을 수 있습니다."  |
| "mc\_sdk\_one\_key\_close\_position" : "원클릭 청산"  |
| "no\_authentication" : "실명인증을 진행해주세요"  |
| "pwd\_rule" : "로그인 비밀 번호는 영문 대소문자 및 숫자를 모두 포함한 8~32자여야 합니다. 로그인 비밀 번호는 거래 비밀 번호랑 같을 수 없습니다."  |
| "pwd\_rule\_contain\_lower" : "비밀번호는 반드시 소문자를 포함해야합니다"  |
| "pwd\_rule\_contain\_number" : "비밀번호는 반드시 숫자를 포함해야합니다"  |
| "pwd\_rule\_contain\_upper" : "비밀번호는 반드시 대문자를 포함해야합니다"  |
| "pwd\_rule\_length" : "비밀번호는 반드시 8-32자리여야 합니다."  |
| "reject\_certificate" : "거절"  |
| "str\_pwd\_tip" : "8-32자리, 영문 대문자 및 소문자, 숫자, 특수 문자 중 2개 이상을 포함해야 합니다"  |
| "str\_pwd\_twice\_verify\_tip" : "두 비밀번호가 일치하지않습니다"  |
| "team\_authentication" : "실명인증 필요합니다"  |
| "team\_invitee\_authentication" : "초대자 실명인증"  |
| "team\_invitee\_need\_authen" : "인증이 필요합니다"  |
| "team\_invitee\_not\_need\_authen" : "인증이 필요없습니다"  |
| "team\_need\_authentication" : "실명인증 필요합니다"  |
| "two\_pwd\_different" : "입력한 비밀번호가 일치하지 않습니다!"  |
| "agree\_certificate" : "Doğrulamayı Kabul Et"  |
| "finish\_auth" : "1. Birinci dereceden toplam %s USDT ile %s USDT değerinde Non-neg Fişi alınabilir. 2. İkinci dereceden toplam %s USDT ile %s USDT değerinde Non-neg Fişi alınabilir."  |
| "mc\_sdk\_one\_key\_close\_position" : "Tek tıkla kapat"  |
| "no\_authentication" : "Henüz gerçek isim doğrulamasını tamamlamadınız"  |
| "pwd\_rule" : "Şifre 8-32 hane arasında olmalıdır, büyük ve küçük harfler ve rakam içermelidir. Giriş şifresi giriş işlem ile aynı olamaz"  |
| "pwd\_rule\_contain\_lower" : "Şifre küçük harf içermelidir"  |
| "pwd\_rule\_contain\_number" : "Şifre rakam içermelidir"  |
| "pwd\_rule\_contain\_upper" : "Şifre büyük harf içermelidir"  |
| "pwd\_rule\_length" : "Şifre 8-31 hane arasında olmalıdır"  |
| "reject\_certificate" : "Doğrulamayı Reddet"  |
| "str\_pwd\_tip" : "8-32 hane arasında olmalıdır; büyük harf, küçük harf, rakam ve en az iki çeşit özel karakter içermelidir."  |
| "str\_pwd\_twice\_verify\_tip" : "Şifreler eşleşmiyor"  |
| "team\_authentication" : "Kimlik Doğrulama"  |
| "team\_invitee\_authentication" : "Davetli Kimlik Doğrulaması"  |
| "team\_invitee\_need\_authen" : "Kimlik doğrulaması gerekiyor"  |
| "team\_invitee\_not\_need\_authen" : "Kimlik doğrulaması gerekmiyor"  |
| "team\_need\_authentication" : "Kimlik doğrulaması gerekiyor"  |
| "two\_pwd\_different" : "Şifreler eşleşmiyor！"  |
| "agree\_certificate" : "Aceita"  |
| "finish\_auth" : "1. A transferência líquida cumulativa de primeiro nível que atinge %sUSDT pode obter um chip não negativo de %sUSDT 2.A transferência líquida cumulativa de segundo nível que atinge %sUSDT pode obter um chip não negativo de %sUSDT"  |
| "mc\_sdk\_one\_key\_close\_position" : "Liquidar"  |
| "no\_authentication" : "Você não concluiu a verificação de identidade"  |
| "pwd\_rule" : "A senha deve ter de 8 a 32 dígitos e conter letras maiúsculas e minúsculas e números. A senha de login não pode ser igual à senha de negociação"  |
| "pwd\_rule\_contain\_lower" : "A senha deve conter letras minúsculas"  |
| "pwd\_rule\_contain\_number" : "A senha deve conter números"  |
| "pwd\_rule\_contain\_upper" : "A senha deve conter letras maiúsculas"  |
| "pwd\_rule\_length" : "A senha deve ter de 8 a 32 dígitos"  |
| "reject\_certificate" : "Recusar"  |
| "str\_pwd\_tip" : "8-32 bits; deve conter inglês maiúsculo e minúsculo, números, caracteres especiais, pelo menos 2 deles."  |
| "str\_pwd\_twice\_verify\_tip" : "Duas senhas inseridas são inconsistentes"  |
| "team\_authentication" : "Autenticação de identidade"  |
| "team\_invitee\_authentication" : "Autenticação do convidado"  |
| "team\_invitee\_need\_authen" : "requer verificação"  |
| "team\_invitee\_not\_need\_authen" : "Nenhuma verificação necessária"  |
| "team\_need\_authentication" : "Autentificação requerida"  |
| "two\_pwd\_different" : "Duas senhas inseridas devem ser consistentes!"  |
| "agree\_certificate" : "Согласиться на верификацию"  |
| "finish\_auth" : "1.Совокупный чистый перевод первого уровня, достигающий %sUSDT может получить %sUSDT Супербонус 2.Совокупный чистый перевод второго уровня, достигающий %sUSDT может получить %sUSDT Супербонуса"  |
| "mc\_sdk\_one\_key\_close\_position" : "Закрыть одним кликом"  |
| "no\_authentication" : "Вы не завершили верификацию личности"  |
| "pwd\_rule" : "Пароль должен состоять из 8-32 символов и содержать прописные и строчные буквы и цифры. Торговый пароль не должен совпадать с паролем входа в систему."  |
| "pwd\_rule\_contain\_lower" : "Пароль должен содержать строчные буквы"  |
| "pwd\_rule\_contain\_number" : "Пароль должен содержать цифры"  |
| "pwd\_rule\_contain\_upper" : "Пароль должен содержать заглавные буквы"  |
| "pwd\_rule\_length" : "Пароль должен состоять из 8-32 символов"  |
| "reject\_certificate" : "Отклонить верификацию"  |
| "str\_pwd\_tip" : "8-32 значный; должен содержать заглавные и строчные буквы английского языка, цифры и специальные символы, по крайней мере 2 из которых."  |
| "str\_pwd\_twice\_verify\_tip" : "Пароли не совпадают"  |
| "team\_authentication" : "Верификация личности"  |
| "team\_invitee\_authentication" : "Верификация личности приглашенных"  |
| "team\_invitee\_need\_authen" : "Требуется верификация"  |
| "team\_invitee\_not\_need\_authen" : "Верификация не требуется"  |
| "team\_need\_authentication" : "Требуется верификация"  |
| "two\_pwd\_different" : "Пароли не совпадают!"  |
| "agree\_certificate" : "同意認證"  |
| "finish\_auth" : "1.一階累計淨劃入%sUSDT可獲得%sUSDT泥碼 2.二階累計淨劃入%sUSDT可獲得%sUSDT泥碼"  |
| "mc\_sdk\_one\_key\_close\_position" : "一鍵平倉"  |
| "no\_authentication" : "您尚未完成實名認證"  |
| "pwd\_rule" : "密碼必須是8-32位，同時包含大小寫字母和數字。登錄密碼不允許與交易密碼一致"  |
| "pwd\_rule\_contain\_lower" : "密碼必須包含小寫字母"  |
| "pwd\_rule\_contain\_number" : "密碼必須包含數字"  |
| "pwd\_rule\_contain\_upper" : "密碼必須包含大寫字母"  |
| "pwd\_rule\_length" : "密碼必須是8-32位"  |
| "reject\_certificate" : "拒絕認證"  |
| "str\_pwd\_tip" : "8-32位，包含大小寫字母和數字"  |
| "str\_pwd\_twice\_verify\_tip" : "兩次密碼不一致"  |
| "team\_authentication" : "身份驗證"  |
| "team\_invitee\_authentication" : "被邀請人身份驗證"  |
| "team\_invitee\_need\_authen" : "需要驗證"  |
| "team\_invitee\_not\_need\_authen" : "不需要驗證"  |
| "team\_need\_authentication" : "需要身份驗證"  |
| "two\_pwd\_different" : "兩次密碼輸入不一致！"  |
| "team\_authentication" : "身份验证"  |
| "team\_invitee\_authentication" : "被邀请人身份验证"  |
| "team\_invitee\_need\_authen" : "需要验证"  |
| "team\_invitee\_not\_need\_authen" : "不需要验证"  |
| "team\_need\_authentication" : "需要身份验证"  |

## **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.HIGH\_SAMPLING\_RATE\_SENSORS | 正常 | 访问更高采样率的传感器数据 | 允许应用访问采样率大于 200 Hz 的传感器数据 |
| 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.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.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| 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.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.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\_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.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.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\_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.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\_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\_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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.NETWORK\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.coinw.weba.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.coinw.weba.andpermission.bridge | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.NFC | 正常 | 控制近场通信 | 允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信 |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| com.coinw.weba.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| cn.cyberidentity.certification.AUTH | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_SETTINGS | 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.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 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 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 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.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| mage.bywop.byw.ui.activity.ThirdLaunchActivity | **Schemes**: coinw://, coinwapp://,  |

**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。**