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

**掌上薪福通（ 5.3.5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 | 掌上薪福通 |
| 版本 | 5.3.5 |
| 包名 | com.cmbchina.xft |
| 域名线索 | 59条 |
| URL线索 | 32条 |
| APP图标 |  |
| 分析日期 | 2025年8月2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 | com.cmbchina.xft\_5.3.5.apk |
| 文件大小 | 101.55MB |
| MD5值 | c562592b044966d5ac1e3a5974fa51b7 |
| SHA1值 | 41eab82e1c751cb60a51cf5e0760f01dfe01aa81 |
| SHA256值 | 489765bd2df9b6a25da56981203f4c1ded2cd27dbacd00bb57ee791c152e5ba9 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 掌上薪福通 |
| 包名 | com.cmbchina.xft |
| 主活动Activity | com.cmbchina.cmf.tabcontent.ui.activity.SplashActivity |
| 安卓版本名称 | 5.3.5 |
| 安卓版本 | 43 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| lf12-32-gateway.paas.cmbchina.com | IP: 58.250.105.1 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| lf12-32-gateway-uat.paasuat.cmbchina.cn | 没有服务器地理信息.  |
| s3gw.cmbchina.com | IP: 58.33.159.185 所属国家: China 地区: Shanghai 城市: Shanghai  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| m.cmbchina.com | IP: 58.33.159.53 所属国家: China 地区: Shanghai 城市: Shanghai  |
| fbuseruat.cmburl.cn | IP: 202.105.111.152 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| url.spec.whatwg.org | IP: 165.227.248.76 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| fbuser.uat.cmbchina.cn | 没有服务器地理信息.  |
| 55.10.46.146 | IP: 55.10.46.146 所属国家: United States of America 地区: Arizona 城市: Fort Huachuca  |
| lf12-32-gateway-st.paasst.cmbchina.cn | 没有服务器地理信息.  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| xft-web-home-cs.paasuat.cmbchina.cn | 没有服务器地理信息.  |
| xft4-web-home-cs.paasuat.cmbchina.cn | 没有服务器地理信息.  |
| xft2-web-home-uat.cmburl.cn | IP: 202.105.111.50 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| xft-demo.cmburl.cn | IP: 202.105.111.77 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| cfs.cmbyc.com | IP: 101.52.252.88 所属国家: China 地区: Beijing 城市: Beijing  |
| xft-web-home-cs.paasst.cmbchina.cn | 没有服务器地理信息.  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| central.jaf.cmbchina.cn | 没有服务器地理信息.  |
| cmb-index.weijuju.com | 没有服务器地理信息.  |
| lf12-32-gateway-dev.paas.cmbchina.cn | 没有服务器地理信息.  |
| www.jsdelivr.com | IP: 172.67.208.113 所属国家: United States of America 地区: California 城市: San Francisco  |
| xft2-web-home-cs.paasst.cmbchina.cn | 没有服务器地理信息.  |
| store-dra.hispace.dbankcloud.com | IP: 222.73.142.47 所属国家: China 地区: Shanghai 城市: Shanghai  |
| eruda.liriliri.io | IP: 172.67.141.185 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| g.co | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| grs.dbankcloud.asia | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| lf12-32-gateway-biz.paas.cmbchina.cn | 没有服务器地理信息.  |
| play.google.com | IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing  |
| xft3-web-home-cs.paasuat.cmbchina.cn | 没有服务器地理信息.  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store-drcn.hispace.dbankcloud.cn | IP: 111.202.17.50 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing  |
| store-drru.hispace.dbankcloud.com | IP: 159.138.201.153 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| lf12-32-gateway-st.csst.cmburl.cn | IP: 202.105.111.3 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| angular.io | IP: 151.101.1.195 所属国家: United States of America 地区: California 城市: San Francisco  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| npms.io | IP: 104.21.32.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| xft.cmbchina.com | IP: 58.33.159.75 所属国家: China 地区: Shanghai 城市: Shanghai  |
| fcstool.paas.cmbchina.cn | 没有服务器地理信息.  |
| xft-web-home-cs.paas.cmbchina.cn | 没有服务器地理信息.  |
| store-dre.hispace.dbankcloud.com | IP: 222.73.142.37 所属国家: China 地区: Shanghai 城市: Shanghai  |
| apimarketgw-test.cmbchina.cn | 没有服务器地理信息.  |
| grs.dbankcloud.cn | IP: 121.36.117.149 所属国家: China 地区: Beijing 城市: Beijing  |
| bit.ly | IP: 67.199.248.11 所属国家: United States of America 地区: New York 城市: New York City  |
| xft-web-home-st.alb-sz.cmburl.cn | 没有服务器地理信息.  |
| lpxwweb.paasst.cmbchina.cn | 没有服务器地理信息.  |
| xft2-web-home-cs.paasuat.cmbchina.cn | 没有服务器地理信息.  |
| fbuser.st.cmbchina.cn | 没有服务器地理信息.  |
| xft6-web-home-cs.paas.cmbchina.cn | 没有服务器地理信息.  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| fbuser.cmbchina.com | IP: 58.33.159.96 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://m.cmbchina.com  | 摸瓜V1引擎  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |
| https://store-drcn.hispace.dbankcloud.cn/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-dra.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-dre.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| https://store-drru.hispace.dbankcloud.com/hwmarket/api/  | 摸瓜V2引擎  |
| http://fcstool.paas.cmbchina.cn/ssoTool/getLoginUrl?empSeqId=  | 摸瓜V2引擎  |
| http://cmf/exitApp  | 摸瓜V2引擎  |
| http://cmf/getUUID  | 摸瓜V2引擎  |
| http://cmf/screenshot  | 摸瓜V2引擎  |
| http://cmf/secureStorage  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://cmf/getWifiInfo  | 摸瓜V2引擎  |
| http://cmf/checkPermission  | 摸瓜V2引擎  |
| http://cmf/bmkGps  | 摸瓜V2引擎  |
| http://cmf/systemSetting  | 摸瓜V2引擎  |
| http://cmf/faceIdentification  | 摸瓜V2引擎  |
| http://cmf/checkPermission  | 摸瓜V2引擎  |
| http://cmf/systemSetting  | 摸瓜V2引擎  |
| http://cmf/exitApp  | 摸瓜V2引擎  |
| http://cmf/gethash  | 摸瓜V2引擎  |
| http://cmf/crypto  | 摸瓜V2引擎  |
| http://cmf/crypto==enc>  | 摸瓜V2引擎  |
| http://cmf/gethash==gethash>  | 摸瓜V2引擎  |
| http://cmf/crypto=dec=>  | 摸瓜V2引擎  |
| http://cmf/uploadPicture  | 摸瓜V2引擎  |
| http://cmf/nativeHttp  | 摸瓜V2引擎  |
| http://cmf/adView  | 摸瓜V2引擎  |
| http://cmf/backAction  | 摸瓜V2引擎  |
| http://cmf/backPressed  | 摸瓜V2引擎  |
| http://cmf/cacheSize  | 摸瓜V2引擎  |
| http://cmf/contactInfo  | 摸瓜V2引擎  |
| http://cmf/deviceInfo  | 摸瓜V2引擎  |
| http://cmf/picture  | 摸瓜V2引擎  |
| http://cmf/gps  | 摸瓜V2引擎  |
| http://cmf/statusbar  | 摸瓜V2引擎  |
| http://cmf/cleanCache  | 摸瓜V2引擎  |
| http://cmf/scanQrCode  | 摸瓜V2引擎  |
| http://cmf/sms  | 摸瓜V2引擎  |
| http://cmf/tel  | 摸瓜V2引擎  |
| http://cmf/lottieLoading  | 摸瓜V2引擎  |
| http://cmf/topBarUI  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://cmf/goBackToRoot  | 摸瓜V2引擎  |
| http://cmf/fingerprintAuth  | 摸瓜V2引擎  |
| http://cmf/replaceRootPage  | 摸瓜V2引擎  |
| https://xft.cmbchina.com/app/  | 摸瓜V2引擎  |
| https://xft.cmbchina.com/  | 摸瓜V2引擎  |
| https://fbuser.cmbchina.com  | 摸瓜V2引擎  |
| http://cmf/genericUI  | 摸瓜V2引擎  |
| http://cmf/xftLogout  | 摸瓜V2引擎  |
| http://cmf/xftNativeIM  | 摸瓜V2引擎  |
| https://npms.io/search?q=ponyfill.  | 摸瓜V2引擎  |
| http://cmf/keyboard  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js/blob/v3.21.1/LICENSE  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js  | 摸瓜V2引擎  |
| http://cmf/getUUID  | 摸瓜V2引擎  |
| http://55.10.46.146  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paas.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paas.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft6-web-home-cs.paas.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft6-web-home-cs.paas.cmbchina.cn/  | 摸瓜V2引擎  |
| https://fbuser.st.cmbchina.cn  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paasst.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paasst.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft2-web-home-cs.paasst.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft2-web-home-cs.paasst.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft-web-home-st.alb-sz.cmburl.cn/app/  | 摸瓜V2引擎  |
| http://xft-web-home-st.alb-sz.cmburl.cn/  | 摸瓜V2引擎  |
| https://fbuseruat.cmburl.cn  | 摸瓜V2引擎  |
| http://xft-demo.cmburl.cn/app/  | 摸瓜V2引擎  |
| http://xft-demo.cmburl.cn/  | 摸瓜V2引擎  |
| https://xft2-web-home-uat.cmburl.cn/app/  | 摸瓜V2引擎  |
| https://xft2-web-home-uat.cmburl.cn/  | 摸瓜V2引擎  |
| https://fbuser.uat.cmbchina.cn  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paasuat.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft-web-home-cs.paasuat.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft2-web-home-cs.paasuat.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft2-web-home-cs.paasuat.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft3-web-home-cs.paasuat.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft3-web-home-cs.paasuat.cmbchina.cn/  | 摸瓜V2引擎  |
| http://xft4-web-home-cs.paasuat.cmbchina.cn/app/  | 摸瓜V2引擎  |
| http://xft4-web-home-cs.paasuat.cmbchina.cn/  | 摸瓜V2引擎  |
| http://cmf/eventHandle  | 摸瓜V2引擎  |
| http://cmf/eventHandleList  | 摸瓜V2引擎  |
| http://g.co/ng/security  | 摸瓜V2引擎  |
| https://angular.io/api/common/NgForOf  | 摸瓜V2引擎  |
| http://cmf/secureStorage  | 摸瓜V2引擎  |
| http://cmf/notificationManager  | 摸瓜V2引擎  |
| http://bit.ly/IWukam  | 摸瓜V2引擎  |
| http://cmf/systemSetting  | 摸瓜V2引擎  |
| http://cmf/screenshot  | 摸瓜V2引擎  |
| http://cmf/secureStorage  | 摸瓜V2引擎  |
| http://cmf/picture  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://apimarketgw-test.cmbchina.cn/uat/10072/around?keywords=kfc&location=113,23&offset=2  | 摸瓜V2引擎  |
| http://cmf/bmkGps  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://cmf/xftNativeIM  | 摸瓜V2引擎  |
| http://cmf/secureStorage  | 摸瓜V2引擎  |
| http://cmf/download  | 摸瓜V2引擎  |
| http://cmf/readDownloadFile  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn  | 摸瓜V2引擎  |
| http://central.jaf.cmbchina.cn:80/artifactory/api/npm/group-npm/@lw36.19/xft-app-web-PRO/-/@lw36.19/xft-app-web-PRO-1.5.20.tgz  | 摸瓜V2引擎  |
| http://cmf/systemSetting  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-uat.paasuat.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-uat.paasuat.cmbchina.cn  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js/blob/v3.32.2/LICENSE  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d?a=1&c=3  | 摸瓜V2引擎  |
| https://a@b  | 摸瓜V2引擎  |
| http://x  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com/front-rest-log/v2/encrypt\_batch\_upload  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.csst.cmburl.cn/front-rest-log/v2/batch\_upload';  | 摸瓜V2引擎  |
| http://cmf/secureStorage',  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn');  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com/front-rest-log/v2/encrypt\_batch\_upload';  | 摸瓜V2引擎  |
| http://cmf/secureStorage',  | 摸瓜V2引擎  |
| http://cmfweb/webviewReturn');  | 摸瓜V2引擎  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | 摸瓜V2引擎  |
| https://eruda.liriliri.io/  | 摸瓜V2引擎  |
| https://github.com/liriliri/eruda  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js/blob/v3.26.1/LICENSE  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js  | 摸瓜V2引擎  |
| https://github.com/WebReflection/url-search-params/blob/master/src/url-search-params.js  | 摸瓜V2引擎  |
| https://url.spec.whatwg.org/  | 摸瓜V2引擎  |
| https://github.com/arv/DOM-URL-Polyfill/blob/master/src/url.js  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d  | 摸瓜V2引擎  |
| http://foo:8080  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.paasst.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.csst.cmburl.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-biz.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway.paas.cmbchina.com  | 摸瓜V2引擎  |
| http://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-dev.paas.cmbchina.cn  | 摸瓜V2引擎  |
| https://lf12-32-gateway-uat.paasuat.cmbchina.cn  | 摸瓜V2引擎  |
| http://lf12-32-gateway-uat.paasuat.cmbchina.cn  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js/blob/v3.32.2/LICENSE  | 摸瓜V2引擎  |
| https://github.com/zloirock/core-js  | 摸瓜V2引擎  |
| http://a  | 摸瓜V2引擎  |
| http://a/c%20d?a=1&c=3  | 摸瓜V2引擎  |
| https://a@b  | 摸瓜V2引擎  |
| http://x  | 摸瓜V2引擎  |
| http://lf12-32-gateway-st.paasst.cmbchina.cn/front-rest-log/v2/batch\_upload  | 摸瓜V2引擎  |
| https://lf12-32-gateway-st.paasst.cmbchina.cn/front-rest-log/v2/batch\_upload  | 摸瓜V2引擎  |
| https://lf12-32-gateway.paas.cmbchina.com/front-rest-log/v2/encrypt\_batch\_upload  | 摸瓜V2引擎  |
| http://lpxwweb.paasst.cmbchina.cn/lpxwmob/index.html  | 摸瓜V2引擎  |
| https://s3gw.cmbchina.com/g/L2x3MzYuMTgtb21zYnVja2V0MS1wcmQvQVRUQTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNzI1NzU\_QVdTQWNjZXNzS2V5SWQ9bHczNi4xOC1vbXN1c2VyMS1wcmQmRXhwaXJlcz0xOTYyNjk2ODA1JlNpZ25hdHVyZT02RGNmJTJCVnk5TlJiMmRSM2dGSmdQSDBFaE80dyUzRA==/vmbY7OI5L559ytgLpY9qBJazkxA=/lw36.18-omsuser1-prd-dmz/1962696805  | 摸瓜V2引擎  |
| https://s3gw.cmbchina.com/g/L2x3MzYuMTgtb21zYnVja2V0MS1wcmQvQVRUQTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNTM5MTk\_QVdTQWNjZXNzS2V5SWQ9bHczNi4xOC1vbXN1c2VyMS1wcmQmRXhwaXJlcz0xOTU2MDQzNzQ3JlNpZ25hdHVyZT10ZyUyQkxqQzBFTmZLSVp1QVJOWWRiMFRmaFFvQSUzRA==/ibImacgKo400ePcPRCHXJpF1UW8=/lw36.18-omsuser1-prd-dmz/1956043747  | 摸瓜V2引擎  |
| https://s3gw.cmbchina.com/g/L2x3MzYuMTgtb21zYnVja2V0MS1wcmQvQVRUQTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNzI1NzU\_QVdTQWNjZXNzS2V5SWQ9bHczNi4xOC1vbXN1c2VyMS1wcmQmRXhwaXJlcz0xOTYyNjk2ODA1JlNpZ25hdHVyZT02RGNmJTJCVnk5TlJiMmRSM2dGSmdQSDBFaE80dyUzRA==/vmbY7OI5L559ytgLpY9qBJazkxA=/lw36.18-omsuser1-prd-dmz/1962696805  | 摸瓜V2引擎  |
| https://s3gw.cmbchina.com/g/L2x3MzYuMTgtb21zYnVja2V0MS1wcmQvQVRUQTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwNTM5MTk\_QVdTQWNjZXNzS2V5SWQ9bHczNi4xOC1vbXN1c2VyMS1wcmQmRXhwaXJlcz0xOTU2MDQzNzQ3JlNpZ25hdHVyZT10ZyUyQkxqQzBFTmZLSVp1QVJOWWRiMFRmaFFvQSUzRA==/ibImacgKo400ePcPRCHXJpF1UW8=/lw36.18-omsuser1-prd-dmz/1956043747  | 摸瓜V2引擎  |
| http://cmbls/functionjump  | 摸瓜V2引擎  |
| https://cmb-index.weijuju.com/4/index.html  | 摸瓜V2引擎  |
| http://cfs.cmbyc.com/h5-app/login  | 摸瓜V2引擎  |
| https://xft.cmbchina.com/m-home/  | 摸瓜V2引擎  |
| https://github.com/opencv/opencv/issues/16739  | lib/armeabi-v7a/libopencv\_java4.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| idcard@1x.png  | 摸瓜V2引擎  |
| arrow-right@2x.png  | 摸瓜V2引擎  |
| close@1x.png back-black@2x.png  | 摸瓜V2引擎  |
| eruda@2.10  | 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: True v3 签名: True 找到 1 个唯一证书 主题: C=cn, ST=shenzhen, L=shenzhen, O=cmbchina, OU=xft, CN=xft 签名算法: rsassa\_pkcs1v15 有效期自: 2021-10-20 09:48:25+00:00 有效期至: 2046-10-14 09:48:25+00:00 发行人: C=cn, ST=shenzhen, L=shenzhen, O=cmbchina, OU=xft, CN=xft 序列号: 0x25c1577b 哈希算法: sha256 md5值: 448efd73ab847415d7508dcd13dfd872 sha1值: ecb337c650cd8644440399ad5add35d786a18cb3 sha256值: 7c0fa770d2167edd44975f34ab2a16c9ec82c135efa35b3f42c831f21199f37f sha512值: 62c527316814511bf532a87c7e2fd181e51cbc27cc066a59c35f5dd7e42f0cfd90eea77cc4d4c9da5a2f92bcb4a32d6d8d07a3d5bb57304d7ff7813f9f12f27c 公钥算法: rsa 密钥长度: 2048 指纹: db1cee1f5bdea8105daabb71346f78e2d05c6f0e5669f07fd6d20d2906f931ca**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "cancel\_more\_auth" : "取消"  |
| "face\_authorized\_msg" : "拒绝人脸识别验证将会无法继续操作，确定拒绝吗？"  |
| "keyboard\_secret" : "配置安全键盘密钥"  |
| "keyboard\_secret\_info" : "自定义安全键盘密钥不能为空"  |
| "login\_pwd" : "密码登录"  |
| "more\_auth\_btn" : "切换账号或登录方式"  |
| "more\_auth\_verify\_btn" : "更多"  |
| "safe\_keyboard\_secret\_title" : "请输入安全键盘密钥"  |
| "xft\_sdk\_get\_session\_failed" : "获取当前会话失败"  |
| "xft\_sdk\_home\_session\_item\_delete" : "删除该聊天"  |
| "xft\_sdk\_home\_session\_item\_delete\_tip" : "删除后，将清空该聊天的消息记录"  |
| "xft\_sdk\_public\_session\_press\_call" : "呼叫"  |
| "xft\_sdk\_public\_session\_press\_copy" : "复制号码"  |
| "xft\_sdk\_public\_session\_press\_phone\_prompt" : "%1$s 可能是一个电话号码，你可以"  |
| "xft\_sdk\_session\_list\_date\_format" : "yyyy年M月d日"  |
| "xft\_sdk\_session\_list\_date\_without\_year\_fromat" : "M月d日"  |
| "keyboard\_secret" : "配置安全鍵盤密鑰"  |
| "keyboard\_secret\_info" : "自定義安全鍵盤密鑰不能為空"  |
| "safe\_keyboard\_secret\_title" : "請輸入安全鍵盤密鑰"  |
| "keyboard\_secret" : "配置安全键盘密钥"  |
| "keyboard\_secret\_info" : "自定义安全键盘密钥不能为空"  |
| "safe\_keyboard\_secret\_title" : "请输入安全键盘密钥"  |

## **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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| 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.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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\_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.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| 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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| com.cmbchina.xft.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| com.cmbchina.xft.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.xft.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.xft.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.pushagent.permission.RICHMEDIA\_PROVIDER | 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.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 |
| com.huawei.launcher3.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher3.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher2.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher2.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher.permission.WRITE\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.xft.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.cmbchina.xft.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.push.permission.READ\_PUSH\_NOTIFICATION\_INFO | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.cmbchina.cmf.tabcontent.ui.activity.PushActivity | **Schemes**: huaweipush://, vpushscheme://, pushscheme://, **Hosts:** com.cmbchina.xft.push.tabcontent, xft.vivo.push, com.honor.push, **Paths:** /notification, /detail, /deeplink,  |
| com.cmbchina.cmf.tabcontent.ui.activity.SchemeActivity | **Schemes**: zsxft://, **Hosts:** startapp,  |

**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。**