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

**自动记账（ 涅槃 3.0.0 beta6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 | 自动记账 |
| 版本 | 涅槃 3.0.0 beta6 |
| 包名 | cn.dreamn.qianji\_auto |
| 域名线索 | 48条 |
| URL线索 | 44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 | 自动记账\_涅槃 3.0.0 beta6.apk |
| 文件大小 | 8.96MB |
| MD5值 | 281fc70f96084fb366666b0b3bc2f0ef |
| SHA1值 | 48f8bd6c972766c77f9f45e43dbfc4149186ac78 |
| SHA256值 | e9ca87aa534d39bb27f8f5c249f4fa1a918ccd2d8b414de06870f0fe0997a3c7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 自动记账 |
| 包名 | cn.dreamn.qianji\_auto |
| 主活动Activity | cn.dreamn.qianji\_auto.ui.activity.MainActivity |
| 安卓版本名称 | 涅槃 3.0.0 beta6 |
| 安卓版本 | 145 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| docs.qianjiapp.com | IP: 114.55.166.105 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| seto.teracloud.jp | IP: 103.139.238.155 所属国家: Japan 地区: Shizuoka 城市: Shizuoka  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| schemas.android.com | 没有服务器地理信息.  |
| underscorejs.org | IP: 172.67.134.18 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ankio.net | IP: 149.104.27.145 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| zenorocha.github.io | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mdn.alipay.com | IP: 116.142.235.232 所属国家: China 地区: Beijing 城市: Beijing  |
| ghproxy.com | IP: 144.24.81.189 所属国家: Korea (Republic of) 地区: Gangwon-do 城市: Chuncheon  |
| java.sun.com | IP: 104.126.37.152 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| pay.weixin.qq.com | IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin  |
| doc.ankio.net | IP: 149.104.27.145 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| player.bilibili.com | IP: 60.213.135.86 所属国家: China 地区: Shandong 城市: Tai'an  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| tutorialzine.com | IP: 104.21.16.1 所属国家: United States of America 地区: California 城市: San Francisco  |
| mmbiz.qpic.cn | IP: 221.204.15.91 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| res.qianjiapp.com | IP: 222.134.1.29 所属国家: China 地区: Shandong 城市: Binzhou  |
| bugs.chromium.org | IP: 142.250.73.83 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.opensource.org | IP: 172.67.26.198 所属国家: United States of America 地区: California 城市: San Francisco  |
| raw.fastgit.org | 没有服务器地理信息.  |
| www.coolapk.com | IP: 60.28.220.193 所属国家: China 地区: Tianjin 城市: Tianjin  |
| jqueryui.com | IP: 104.18.228.34 所属国家: United States of America 地区: California 城市: San Francisco  |
| famspam.com | IP: 165.160.15.20 所属国家: United States of America 地区: Delaware 城市: Wilmington  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| cdn.jsdelivr.net | IP: 104.16.174.226 所属国家: United States of America 地区: California 城市: San Francisco  |
| codemirror.net | IP: 149.210.142.219 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| wx.tenpay.com | IP: 220.196.148.65 所属国家: China 地区: Jiangsu 城市: Yancheng  |
| render.alipay.com | IP: 124.165.219.237 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| pubdav.ctfile.com | IP: 124.160.151.82 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| marijnhaverbeke.nl | IP: 149.210.142.219 所属国家: Netherlands 地区: Noord-Holland 城市: Amsterdam  |
| webdav.ctfile.com | IP: 124.160.151.82 所属国家: China 地区: Zhejiang 城市: Jiaxing  |
| raw.githubusercontent.com | IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| pic.dreamn.cn | IP: 222.134.1.28 所属国家: China 地区: Shandong 城市: Binzhou  |
| snsauth.ccb.com | IP: 111.205.126.90 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| qr.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| payapp.weixin.qq.com | IP: 220.194.111.104 所属国家: China 地区: Tianjin 城市: Tianjin  |
| jshint.com | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| open.weixin.qq.com | IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai  |
| material.io | IP: 216.239.32.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| swiperjs.com | IP: 104.21.29.86 所属国家: United States of America 地区: California 城市: San Francisco  |
| support.weixin.qq.com | IP: 182.50.12.232 所属国家: China 地区: Beijing 城市: Beijing  |
| dav.jianguoyun.com | IP: 103.52.173.35 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://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png  | cn/dreamn/qianji\_auto/database/Helper/Category.java  |
| https://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png  | cn/dreamn/qianji\_auto/database/Helper/CategoryNames.java  |
| https://pic.dreamn.cn/uPic/2021032314475916164820791616482079785ssWEen  | cn/dreamn/qianji\_auto/database/Helper/CategoryNames.java  |
| https://pic.dreamn.cn/uPic/2021032022075916162492791616249279427UY2ok6  | cn/dreamn/qianji\_auto/database/Helper/Assets.java  |
| http://res.qianjiapp.com/headerimages2/maarten-van-den-heuvel-7RyfX2BHoXU-unsplash.jpg!headerimages2  | cn/dreamn/qianji\_auto/database/Helper/BookNames.java  |
| https://qr.alipay.com/fkx18202qn4k2xono9fjk2f  | cn/dreamn/qianji\_auto/utils/supportUtils/DonateUtil.java  |
| https://seto.teracloud.jp/dav/  | cn/dreamn/qianji\_auto/utils/files/BackupManager.java  |
| https://pubdav.ctfile.com/  | cn/dreamn/qianji\_auto/utils/files/BackupManager.java  |
| https://webdav.ctfile.com/  | cn/dreamn/qianji\_auto/utils/files/BackupManager.java  |
| https://dav.jianguoyun.com/dav/  | cn/dreamn/qianji\_auto/utils/files/BackupManager.java  |
| https://cdn.jsdelivr.net/gh/dreamncn/AutoResource@master  | cn/dreamn/qianji\_auto/ui/utils/AutoBillWeb.java  |
| https://ghproxy.com/https://raw.githubusercontent.com/dreamncn/AutoResource/master  | cn/dreamn/qianji\_auto/ui/utils/AutoBillWeb.java  |
| https://raw.githubusercontent.com/dreamncn/AutoResource/master  | cn/dreamn/qianji\_auto/ui/utils/AutoBillWeb.java  |
| https://raw.fastgit.org/dreamncn/AutoResource/master  | cn/dreamn/qianji\_auto/ui/utils/AutoBillWeb.java  |
| https://pic.dreamn.cn/uPic/2021032310470716164676271616467627123WiARFwd8b1f5bdd0fca9378a915d8531cb740b.png  | cn/dreamn/qianji\_auto/ui/fragment/base/sorts/sortsFragment.java  |
| https://pic.dreamn.cn/uPic/2021032022075916162492791616249279427UY2ok6  | cn/dreamn/qianji\_auto/ui/fragment/base/cards/assertFragment.java  |
| https://www.ankio.net  | cn/dreamn/qianji\_auto/ui/fragment/about/DevsFragment.java  |
| https://doc.ankio.net/doc/%E8%87%AA%E5%8A%A8%E8%AE%B0%E8%B4%A6%E4%BD%BF%E7%94%A8%E6%96%87%E6%A1%A3/  | cn/dreamn/qianji\_auto/ui/fragment/about/AboutFragment.java  |
| https://www.coolapk.com/apk/cn.dreamn.qianji\_auto  | cn/dreamn/qianji\_auto/ui/fragment/about/AboutFragment.java  |
| http://docs.qianjiapp.com/plugin/auto\_tasker.html  | cn/dreamn/qianji\_auto/core/hook/app/qianji/hooks/AutoError.java  |
| https://material.io/design/components/dialogs.html  | com/afollestad/materialdialogs/MaterialDialog.java  |
| http://java.sun.com/xml/stream/properties/report-cdata-event  | com/bea/xml/stream/ConfigurationContextBase.java  |
| http://c  | com/bea/xml/stream/XMLWriterBase.java  |
| http://d  | com/bea/xml/stream/XMLWriterBase.java  |
| http://e  | com/bea/xml/stream/XMLWriterBase.java  |
| http://f  | com/bea/xml/stream/XMLWriterBase.java  |
| http://xmlpull.org/v1/doc/features.html  | com/bea/xml/stream/MXParser.java  |
| http://java.sun.com/xml/stream/properties/report-cdata-event  | com/bea/xml/stream/MXParser.java  |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/PermissionChecker.java  |
| http://schemas.android.com/android/skin  | com/zhengsr/skinlib/SkinConstants.java  |
| http://xml.apache.org/xslt  | fr/arnaudguyon/xmltojsonlib/JsonToXml.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| http://127.0.0.1  | org/mozilla/javascript/tools/debugger/Dim.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://javax.xml.XMLConstants/property/accessExternalDTD  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/mxp1\_serializer/MXSerializer.java  |
| http://xmlpull.org/v1/doc/properties.html  | org/xmlpull/mxp1\_serializer/MXSerializer.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/v1/XmlPullParserFactory.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/v1/XmlPullParser.java  |
| http://xmlpull.org/v1/doc/properties.html  | org/xmlpull/v1/builder/impl/XmlPullBuilderImpl.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/v1/wrapper/classic/StaticXmlSerializerWrapper.java  |
| http://apache.org/xml/features/validation/dynamic  | org/xmlpull/v1/sax2/Driver.java  |
| http://apache.org/xml/features/validation/schema  | org/xmlpull/v1/sax2/Driver.java  |
| http://xml.org/sax/properties/declaration-handler  | org/xmlpull/v1/sax2/Driver.java  |
| http://xml.org/sax/properties/lexical-handler  | org/xmlpull/v1/sax2/Driver.java  |
| http://xml.org/sax/features/namespaces  | org/xmlpull/v1/sax2/Driver.java  |
| http://xml.org/sax/features/namespace-prefixes  | org/xmlpull/v1/sax2/Driver.java  |
| http://xml.org/sax/features/validation  | org/xmlpull/v1/sax2/Driver.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/v1/sax2/Driver.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/mxp1/MXParser.java  |
| http://xmlpull.org/v1/doc/properties.html  | org/xmlpull/mxp1/MXParser.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/mxp1/MXParserCachingStrings.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/mxp1/MXParserNonValidating.java  |
| https://player.bilibili.com/player.html?aid=289448844&bvid=BV1Hf4y147Yi&cid=303785417&page=1  | 摸瓜V1引擎  |
| https://github.com/dreamncn/Qianji\_auto  | 摸瓜V1引擎  |
| https://github.com/dreamncn/Qianji\_auto/issues  | 摸瓜V1引擎  |
| https://doc.ankio.net/doc/%E8%87%AA%E5%8A%A8%E8%AE%B0%E8%B4%A6%E4%BD%BF%E7%94%A8%E6%96%87%E6%A1%A3/  | 摸瓜V1引擎  |
| https://codemirror.net/LICENSE  | 摸瓜V2引擎  |
| https://codemirror.net),  | 摸瓜V2引擎  |
| http://marijnhaverbeke.nl/blog/  | 摸瓜V2引擎  |
| http://unicode.org/reports/tr9/tr9-13.html  | 摸瓜V2引擎  |
| https://github.com/codemirror/CodeMirror/pull/5673  | 摸瓜V2引擎  |
| https://bugs.chromium.org/p/chromium/issues/detail?id=489206  | 摸瓜V2引擎  |
| http://marijnhaverbeke.nl/blog/codemirror-line-tree.html  | 摸瓜V2引擎  |
| https://codemirror.net/LICENSE  | 摸瓜V2引擎  |
| http://jshint.com/docs/options/  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2277  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2534  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/issues/2559  | 摸瓜V2引擎  |
| https://github.com/highlightjs/highlight.js/pull/2844  | 摸瓜V2引擎  |
| http://jqueryui.com  | 摸瓜V2引擎  |
| http://underscorejs.org  | 摸瓜V2引擎  |
| http://famspam.com/facebox/  | 摸瓜V2引擎  |
| http://www.opensource.org/licenses/mit-license.php  | 摸瓜V2引擎  |
| https://zenorocha.github.io/clipboard.js  | 摸瓜V2引擎  |
| http://tutorialzine.com/2012/02/enhance-your-website-fullscreen-api/  | 摸瓜V2引擎  |
| http://swiperjs.com  | 摸瓜V2引擎  |
| https://render.alipay.com/p/f/fd-jblxfp45/pages/home/index.html,topSubContent:  | 摸瓜V2引擎  |
| https://mdn.alipay.com/wsdk/img?fileid=A\*ebkWSJ9yja0AAAAAAAAAAAAAAfYuAQ&bz=life\_app&zoom=2048w\_80q\_1l,link:alipays://platformapi/startapp?appId=20000032&isOpenedFund=true&tagid=YEB\_INTEREST\_INCOME\_NOTIFY,assistName1:  | 摸瓜V2引擎  |
| https://mdn.alipay.com/wsdk/img?fileid=A\*ebkWSJ9yja0AAAAAAAAAAAAAAfYuAQ&bz=life\_app&zoom=2048w\_80q\_1l,sceneExtInfo:,sceneTitle:  | 摸瓜V2引擎  |
| https://mdn.alipay.com/wsdk/img?fileid=A\*K\_cbS69OOIMAAAAAAAAAAABkAfYuAQ&bz=life\_app&zoom=2048w\_80q\_1l,sceneExtInfo:vipMsgNoteType:number,isProhibited:false,vip:1,sceneTitle:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,soundtype:0,mmreader:template\_detail:template\_show\_type:1,text\_content:cover:,color:,text:,new\_tmpl\_type:0,line\_content:topline:value:color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:,weapp\_username:,op\_type:0,is\_rich\_text:0,word:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,icon\_url:http://mmbiz.qpic.cn/mmbiz\_png/8SAQkPMWIYB1uPsVlhric5TuWs4EPoHEjbadav39ic45Oc4ibRKuIyOWuYvnicsx25ITnF37cmuULHzicK3wHkQuiagQ/640?wx\_fmt=png&wxfrom=200,transaction\_id:4200001204202110013525414437,first\_color:,title\_color:,pay\_style:1,finder\_user\_name:,pub\_time:1633095300,header\_jump\_type:0,show\_right\_icon\_and\_desc\_name:0,display\_name:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=4200001204202110013525414437&accid=085e9858ea81e8ed9d0361ea0,tweetid:,play\_length:0,comment\_topic\_id:0,music\_source:0,longurl:,styles:topColor:,style:[color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,soundtype:0,mmreader:template\_detail:template\_show\_type:1,text\_content:cover:,color:,text:,new\_tmpl\_type:0,line\_content:topline:value:color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:,weapp\_username:,op\_type:0,is\_rich\_text:0,word:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100010710121100600060321701373525743&accid=085e9858ebb18158374fa8bef,tweetid:,play\_length:0,comment\_topic\_id:0,music\_source:0,longurl:,styles:topColor:,style:[color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/userroll/readtemplate?t=userroll/index\_tmpl&type=userrolldetail&trans\_id=4200001200202109299385358329&create\_time=1632885054,soundtype:0,mmreader:template\_detail:template\_show\_type:1,text\_content:cover:,color:,text:,new\_tmpl\_type:0,line\_content:topline:value:color:  | 摸瓜V2引擎  |
| https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx57849631bb367f52&response\_type=code&scope=snsapi\_base&state=1&redirect\_uri=https%3A%2F%2Fpay.weixin.qq.com%2Faction%2Findex.php%2Fmmpayentrustweb%2Fentrustweb%2Fmanager\_contract%3Ftarget\_page%3Ddetail%26contract\_no%3D202102245742457281%26mer\_code%3D1300516601%26from%3Dtemp\_msg%26source%3D3,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:,weapp\_username:,op\_type:0,is\_rich\_text:0,word:  | 摸瓜V2引擎  |
| https://pay.weixin.qq.com/mmpaykf/faqmanage?ver=v1&trans\_id=4200001200202109299385358329&create\_time=1632885054&wx\_header=0&scene\_code=payproof\_cell,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:,weapp\_username:,op\_type:0,is\_rich\_text:0,word:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/userroll/readtemplate?t=userroll/index\_tmpl&type=userrolldetail&trans\_id=4200001200202109299385358329&create\_time=1632885054,tweetid:,play\_length:0,comment\_topic\_id:0,music\_source:0,longurl:,styles:topColor:,style:[color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,soundtype:0,mmreader:template\_detail:template\_show\_type:1,text\_content:cover:,color:,text:,new\_tmpl\_type:0,line\_content:topline:value:color:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:,weapp\_username:,op\_type:0,is\_rich\_text:0,word:  | 摸瓜V2引擎  |
| https://payapp.weixin.qq.com/qrpay/qrapph5/merchant/info?outtradeno=10000499012021092901324243191507,weapp\_version:0,ext\_id:,is\_show\_red\_dot:0,hint\_word:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,icon\_url:https://wx.gtimg.com/resource/feuploader/202104/2083e7a5d5b76933c4f32dee47b88571\_128x128.jpg,transaction\_id:10000499012021092901324243191507,first\_color:,title\_color:,pay\_style:1,finder\_user\_name:,pub\_time:1632917002,header\_jump\_type:2,show\_right\_icon\_and\_desc\_name:0,display\_name:  | 摸瓜V2引擎  |
| https://wx.tenpay.com/cgi-bin/mmpayweb-bin/jumpuserroll?trans\_id=100004990121092900060321905318676247&accid=085e9858e772ddcd0f08c3dd6,tweetid:,play\_length:0,comment\_topic\_id:0,music\_source:0,longurl:,styles:topColor:,style:[color:  | 摸瓜V2引擎  |
| https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common\_page\_\_upgrade&text=text001&btn\_text=btn\_text\_0,status:2,cache\_money:  | 摸瓜V2引擎  |
| https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common\_page\_\_upgrade&text=text001&btn\_text=btn\_text\_0,content:,url:https://support.weixin.qq.com/cgi-bin/mmsupport-bin/readtemplate?t=page/common\_page\_\_upgrade&text=text001&btn\_text=btn\_text\_0,status:3,cache\_money:  | 摸瓜V2引擎  |
| https://snsauth.ccb.com/msg\_adapter/stat\_click?openid=o8QqFjln3ubk63rhXDS4dxub43Aw&actId=SSZ32020210915183558849&tailId=TAIL\_000000174320&msgType=3&headers=ygn73wgUxk%2BeeuYpySmd80e6uuS0jvgFJySwSN3%2FywVaRPfwE9ombRHzrLbt08b1WBXY2FEf%2B3id2J5bCvVHlt5Q0RCchA8QFMiaxRk%2FPi09y0tTalK%2Fo5JANgblsdrnG%2BWELlwTQoYyGgputvVQyw%3D%3D  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| chris@ozmm.org jason@onehackoranother.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=99, ST=dreamn, L=dreamn, O=dreamn, OU=dreamn, CN=dreamn 签名算法: rsassa\_pkcs1v15 有效期自: 2020-03-26 14:42:51+00:00 有效期至: 2045-03-20 14:42:51+00:00 发行人: C=99, ST=dreamn, L=dreamn, O=dreamn, OU=dreamn, CN=dreamn 序列号: 0x756e4126 哈希算法: sha256 md5值: b0c9c2225d55202b606f2b145f4465bd sha1值: 18c8228dcfe096491a15980b479bb89217505704 sha256值: 95dff92073e5241ce0f90a0c34e244287779a4ea3b0b02ec0c5911a031e235bf sha512值: 8694424433349394304e9cbf2ea929175739f160853c8c85974c266cd4eb88362d45bc531770a956a301b08d1a2517b65eb05d11dc967b4bfbf3494b1fa681aa 公钥算法: rsa 密钥长度: 2048 指纹: be00fe64ab7097fcd43656d8996ba87313ed48079eb34376ff2a761996c2c8e3**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dev\_user" : "开发人员"  |
| "webdav\_user" : "WebDav用户名"  |

## **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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| 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.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 |
| 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\_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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |

## **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。**