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

**码库（ 4.0.6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 | 码库 |
| 版本 | 4.0.6 |
| 包名 | xyz.foil.teyelf |
| 域名线索 | 37条 |
| URL线索 | 46条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | uetoken-xyz.foil.teyelf.apk |
| 文件大小 | 33.79MB |
| MD5值 | 626ea3a9a14eb6b3a236f86b7ff0b61a |
| SHA1值 | 8f1550f86ee0e5db8bd335960db552c6980b8090 |
| SHA256值 | 13bf48166d9c591dbfb9066b84f59b6c8fe90162bb7eddd8382768fbec573a17 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 码库 |
| 包名 | xyz.foil.teyelf |
| 主活动Activity | com.uetoken.cn.mvp.ui.activity.SplashActivity |
| 安卓版本名称 | 4.0.6 |
| 安卓版本 | 106 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ucc.umeng.com | IP: 203.119.169.175  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| uev2.dtwy.xyz | IP: 116.213.43.145  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| errlogos.umeng.com | IP: 47.246.110.18  所属国家: Singapore  地区: Singapore  城市: Singapore |
| utoken.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |
| log.tbs.qq.com | IP: 124.95.231.218  所属国家: China  地区: Liaoning  城市: Shenyang |
| errnewlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| resolve.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pslog.umeng.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| tbs.imtt.qq.com | IP: 122.188.45.181  所属国家: China  地区: Hubei  城市: Jingzhou |
| cnlogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| schemas.android.com | 没有服务器地理信息. |
| mdc.html5.qq.com | IP: 125.39.196.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| accounts.google.com | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| support.metamask.io | IP: 173.252.108.21  所属国家: United States of America  地区: California  城市: Menlo Park |
| ulogs.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| alogus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| errnewlog.umeng.com | IP: 223.109.148.129  所属国家: China  地区: Jiangsu  城市: Nanjing |
| developer.umeng.com | IP: 59.82.60.43  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| help.tpwallet.io | IP: 202.53.137.209  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| api.github.com | IP: 20.205.243.168  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errlog.umeng.com | IP: 223.109.148.142  所属国家: China  地区: Jiangsu  城市: Nanjing |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| d30bkbk9zem6y9.cloudfront.net | IP: 108.157.254.100  所属国家: United States of America  地区: Washington  城市: Seattle |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| alogsus.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| greenrobot.org | IP: 85.13.163.69  所属国家: Germany  地区: Thuringen  城市: Friedersdorf |
| pms.mb.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| s3-us-west-1.amazonaws.com | IP: 52.219.120.216  所属国家: United States of America  地区: California  城市: San Jose |
| cfg.imtt.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| res.ue.shumaoheng.com | IP: 47.97.231.117  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| client.ue.shumaoheng.com | IP: 47.97.231.117  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| aspect-upush.umeng.com | IP: 223.109.148.141  所属国家: China  地区: Jiangsu  城市: Nanjing |
| unpkg.com | IP: 104.18.1.22  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://s3-us-west-1.amazonaws.com | com/amazonaws/services/s3/AmazonS3Client.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/y.java |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://)([\\s\\S]+) | com/huawei/hms/scankit/p/t3.java |
| https://github.com/kongzue/DialogX/wiki | com/kongzue/dialogx/DialogX.java |
| https://github.com/kongzue/DialogX | com/kongzue/dialogx/interfaces/BaseDialog.java |
| https://github.com/kongzue/DialogX/wiki | com/kongzue/dialogx/interfaces/l.java |
| https://github.com/kongzue/DialogX | com/kongzue/filedialog/FileDialog.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/k.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/o.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/o.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/o.java |
| https://tbs.imtt.qq.com/plugin/DebugPlugin\_v2.tbs | com/tencent/smtt/utils/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://api.github.com | com/uetoken/cn/mvp/model/api/Api.java |
| https://uev2.dtwy.xyz | com/uetoken/cn/mvp/model/api/Api.java |
| http://client.ue.shumaoheng.com | com/uetoken/cn/mvp/model/api/Api.java |
| https://d30bkbk9zem6y9.cloudfront.net/uev2/0.json | com/uetoken/cn/mvp/model/api/Api.java |
| https://d30bkbk9zem6y9.cloudfront.net/uev2/0\_test.json | com/uetoken/cn/mvp/model/api/Api.java |
| https://unpkg.com/vconsole@latest/dist/vconsole.min.js';script.onload | com/uetoken/cn/mvp/ui/tencentx5/X5WebViewActivity.java |
| http://res.ue.shumaoheng.com/ueres/test/uejstest.html | com/uetoken/cn/mvp/ui/activity/me/AboutUsActivity.java |
| https://support.metamask.io/zh-cn/managing-my-tokens/custom-tokens/how-to-display-tokens-in-metamask/ | com/uetoken/cn/mvp/ui/activity/dtc/DtcPublicChainActivity.java |
| https://help.tpwallet.io/cn/wallet-management/token/about-custom-token | com/uetoken/cn/mvp/ui/activity/dtc/DtcPublicChainActivity.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/l.java |
| https://aspect-upush.umeng.com/occa/v1/event/report | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/ext\_event | com/umeng/analytics/pro/aq.java |
| https://cnlogs.umeng.com/uapp\_ekverr\_logs | com/umeng/analytics/pro/aq.java |
| https://resolve.umeng.com/resolve | com/umeng/analytics/pro/by.java |
| https://ucc.umeng.com/v2/inn/fetch | com/umeng/analytics/pro/ar.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 |
| https://developer.umeng.com/docs/119267/detail/118637 | com/umeng/commonsdk/debug/UMLogCommon.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://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://utoken.umeng.com | com/umeng/umzid/ZIDManager.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Completable.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Single.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/Maybe.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://schemas.android.com/apk/res/android | i4/b.java |
| http://www.slf4j.org/codes.html | hg/b.java |
| https://greenrobot.org/greendao/documentation/database-encryption/ | org/greenrobot/greendao/database/DatabaseOpenHelper.java |
| http://xml.apache.org/xslt | n5/b.java |
| https://accounts.google.com/o/oauth2/v2/auth | e9/b.java |
| https://uev2.dtwy.xyz/home/googleauth | e9/b.java |
| https://api.github.com/ | f5/q.java |
| https://github.com/kongzue/DialogX | u5/a.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| x5tbs@tencent.com | com/tencent/smtt/sdk/X5Downloader.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15107301212 | wa/e0.java |
| 15107301212 | wa/o.java |
| 15107301212 | wa/w0.java |

## **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=China, ST=China, L=China, O=China, OU=China, CN=China 签名算法: rsassa\_pkcs1v15 有效期自: 2023-11-22 09:21:03+00:00 有效期至: 2078-08-25 09:21:03+00:00 发行人: C=China, ST=China, L=China, O=China, OU=China, CN=China 序列号: 0x1b2a8a2d2df746bf 哈希算法: sha256 md5值: 799bdabe869f46e1255ebf22834e7420 sha1值: 88992718d6c939a22f89f4979feaf2f519a4a499 sha256值: 9c65643c3a3f0c0fdcf9aa87d23e63372b51c42fa09153098c3031bd6f8914b9 sha512值: a2aa136814d5f44d3546af53432b15f513ade41d7db69b0283f47fb621272ab8ae4d33ae69adb559be1c57def0f31afc3f9e946a1139cd95e3448eefc2f10b47 公钥算法: rsa 密钥长度: 2048 指纹: 253b34f6e924674f0e22cb6a407623e6e4c24592e3fe023c6af74683fafe24c3**

## **6. 硬编码敏感信息**

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.READ\_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\_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.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.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.BLUETOOTH\_SCAN | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_ADVERTISE | 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.uetoken.cn.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.uetoken.cn.mvp.ui.activity.SplashActivity | **Schemes**: ue://, uepay://, |
| com.uetoken.cn.google.GoogleAuthCallbackActivity | **Schemes**: https://,  **Hosts:** uev2.dtwy.xyz,  **Path Prefixes:** /home/googleauth, |

**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。**