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

**U16.com（ 4.8.1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 | U16.com |
| 版本 | 4.8.1 |
| 包名 | com.u166.mmlv |
| 域名线索 | 26条 |
| URL线索 | 16条 |
| APP图标 |  |
| 分析日期 | 2024年10月30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 | zzzzzz11.apk |
| 文件大小 | 34.0MB |
| MD5值 | fb238eba75da221f32d09fcbcdff6f0f |
| SHA1值 | 9db5979e5e43f92ab3c19954c3d3e7f8e3e7f49d |
| SHA256值 | 2de6af2163cb1d02806f09f9cba075724f383cbbc9515c747675f70e719edfc7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | U16.com |
| 包名 | com.u166.mmlv |
| 主活动Activity | com.momo.live.MainActivity |
| 安卓版本名称 | 4.8.1 |
| 安卓版本 | 481 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| s3.kpabe.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| s3.polarcloud.cc | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.unicode.org | IP: 64.182.27.164 所属国家: United States of America 地区: Texas 城市: Dallas  |
| oss.xietch.com | IP: 18.172.52.63 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.wireless-village.org | IP: 172.67.131.214 所属国家: United States of America 地区: California 城市: San Francisco  |
| verify.xietch.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.openmobilealliance.org | IP: 104.26.8.105 所属国家: United States of America 地区: California 城市: San Francisco  |
| s3.polardata.cc | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| s3.polarmeta.cc | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| newh5.xietch.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| s3.xietch.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| www.example.com | IP: 93.184.215.14 所属国家: United States of America 地区: California 城市: Los Angeles  |
| developer.android.com | IP: 172.217.14.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| momo.com | IP: 35.169.254.230 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| s3.anyixs.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| rtc.xietch.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| s3.trfcls.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| java.xietch.com | IP: 156.59.153.67 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| dartbug.com | IP: 216.239.36.21 所属国家: United States of America 地区: California 城市: Mountain View  |
| docs.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/Baseflow/flutter-permission-handler/issues  | com/baseflow/permissionhandler/PermissionManager.java  |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview\_android/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://momo.com  | com/momo/live/http/ReleaseServer.java  |
| https://docs.flutter.dev/deployment/android  | io/flutter/embedding/engine/loader/FlutterLoader.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| http://www.wireless-village.org/CSP  | org/kxml2/wap/wv/WV.java  |
| http://www.wireless-village.org/PA  | org/kxml2/wap/wv/WV.java  |
| http://www.wireless-village.org/TRC  | org/kxml2/wap/wv/WV.java  |
| http://www.openmobilealliance.org/DTD/WV-CSP  | org/kxml2/wap/wv/WV.java  |
| http://www.openmobilealliance.org/DTD/WV-PA  | org/kxml2/wap/wv/WV.java  |
| http://www.openmobilealliance.org/DTD/WV-TRC  | org/kxml2/wap/wv/WV.java  |
| http://www.  | org/kxml2/wap/wml/Wml.java  |
| https://www.  | org/kxml2/wap/wml/Wml.java  |
| http://xmlpull.org/v1/doc/features.html  | org/kxml2/io/KXmlSerializer.java  |
| http://xmlpull.org/v1/doc/  | org/kxml2/io/KXmlParser.java  |
| http://xmlpull.org/v1/doc/properties.html  | org/kxml2/kdom/Document.java  |
| http://xmlpull.org/v1/doc/features.html  | org/xmlpull/v1/XmlPullParser.java  |
| https://github.com/richtr/NoSleep.js/issues/15  | 摸瓜V2引擎  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | 摸瓜V2引擎  |
| https://s3.polardata.cc/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://rtc.xietch.com  | lib/armeabi-v7a/libapp.so  |
| https://developer.mozilla.org/en-US/docs/Web/HTTP/Status  | lib/armeabi-v7a/libapp.so  |
| https://s3.trfcls.com/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://oss.xietch.com  | lib/armeabi-v7a/libapp.so  |
| https://s3.anyixs.com/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://s3.polarmeta.cc/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://s3.kpabe.com/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://s3.xietch.com/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://github.com/dart-lang/language/issues/3488  | lib/armeabi-v7a/libapp.so  |
| https://newh5.xietch.com  | lib/armeabi-v7a/libapp.so  |
| https://java.  | lib/armeabi-v7a/libapp.so  |
| https://java.xietch.com  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://s3.polarcloud.cc/firebase/momo\_domain.txt  | lib/armeabi-v7a/libapp.so  |
| https://verify.xietch.com  | lib/armeabi-v7a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/armeabi-v7a/libflutter.so  |
| https://docs.flutter.dev/release/breaking-changes/android-surface-plugins  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://dartbug.com/52121.  | lib/armeabi-v7a/libflutter.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/arm64-v8a/libapp.so  |
| http://www.unicode.org/copyright.html  | lib/arm64-v8a/libflutter.so  |
| https://docs.flutter.dev/release/breaking-changes/android-surface-plugins  | lib/arm64-v8a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/arm64-v8a/libflutter.so  |
| https://dartbug.com/52121.  | lib/arm64-v8a/libflutter.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| \_nativesocket@14069316.listen \_httpparser@13463476.responsepa \_internetaddress@14069316.fixed \_double@0150898.fromintege \_future@4048458.immediate \_growablelist@0150898.\_literal \_pointerpanzoomdata@387213599.fromupdate \_link@14069316.fromrawpat \_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec \_colorfilter@15065589.mode \_imagefilter@15065589.composed \_list@0150898.\_ofarray \_timer@1026248.periodic \_growablelist@0150898.\_literal2 \_bigintimpl@0150898.from storationinformation@259124995.fromserial \_list@0150898.empty \_directory@14069316.fromrawpat \_invocationmirror@0150898.\_withtype \_colorfilter@15065589.lineartosr \_uri@0150898.file \_growablelist@0150898.\_literal1 \_imagefilter@15065589.blur \_growablelist@0150898.\_literal4 \_growablelist@0150898.\_ofgrowabl \_growablelist@0150898.of \_assetmanifestbin@49287047.fromstanda authenticationscheme@13463476.fromstring \_list@0150898.of \_list@0150898.generate \_typeerror@0150898.\_create \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_routedata@1016504625.ofroute \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 \_growablelist@0150898.\_ofother \_future@4048458.value \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_list@0150898.\_ofother \_bytebuffer@7027147.\_new \_compressednode@41137193.single ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create \_nativesocket@14069316.normal \_imagefilter@15065589.fromcolorf \_colorfilter@15065589.srgbtoline \_uri@0150898.directory \_httpparser@13463476.requestpar \_growablelist@0150898.\_literal8 \_file@14069316.fromrawpat \_growablelist@0150898.generate \_uri@0150898.notsimple \_growablelist@0150898.\_literal7 \_future@4048458.zonevalue \_growablelist@0150898.\_ofefficie \_future@4048458.immediatee \_hashcollisionnode@41137193.fromcollis  | lib/armeabi-v7a/libapp.so  |
| \_growablelist@0150898.\_literal2  | lib/arm64-v8a/libapp.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**无法读取代码签名证书.**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.WRITE\_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.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.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 |
| com.u166.mmlv.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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。 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**