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

**Citadel（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 | Citadel |
| 版本 |  |
| 包名 | com.tl2830284.rf8754552 |
| 域名线索 | 15条 |
| URL线索 | 28条 |
| APP图标 |  |
| 分析日期 | 2024年9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 | com.tl2830284.rf8754552.apk |
| 文件大小 | 129.32MB |
| MD5值 | d5dcb078df2e350fce11e681a992be6c |
| SHA1值 | 8d701057dab9053277b914b99df1303a22717948 |
| SHA256值 | c93d4d0c380c6a90846c51e4919ae46dd285bfc205525d1c877d01219a5d33ff |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Citadel |
| 包名 | com.tl2830284.rf8754552 |
| 主活动Activity |  |
| 安卓版本名称 |  |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.twolame.org | IP: 93.93.131.3 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Cambridge  |
| ultravideo.cs.tut.fi | IP: 130.230.203.118 所属国家: Finland 地区: Pirkanmaa 城市: Tampere  |
| stackoverflow.com | IP: 172.64.155.249 所属国家: United States of America 地区: California 城市: San Francisco  |
| www.ffmpeg.org | IP: 79.124.17.100 所属国家: Bulgaria 地区: Sofia (stolitsa) 城市: Sofia  |
| www.oasis-open.org | IP: 172.99.100.168 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| paulbakaus.com | IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton  |
| www.gnu.org | IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| dev.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| developer.android.com | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| lame.sf.net | IP: 104.18.21.237 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  |
| android.googlesource.com | IP: 74.125.204.82 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  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://www.example.com  | com/pichillilorenzo/flutter\_inappwebview/chrome\_custom\_tabs/CustomTabsHelper.java  |
| https://github.com/pichillilorenzo/flutter\_inappwebview  | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects\n\n\n  | com/pichillilorenzo/flutter\_inappwebview/in\_app\_webview/FlutterWebView.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://github.com/flutter/flutter/issues/2897).It  | io/flutter/plugin/platform/PlatformViewsController.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| https://github.com/flutter/flutter/wiki/Upgrading-pre-1.12-Android-projects  | io/flutter/view/FlutterView.java  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| https://www.gnu.org/licenses/>.  | 摸瓜V2引擎  |
| http://paulbakaus.com/tutorials/html5/web-audio-on-ios/  | 摸瓜V2引擎  |
| http://stackoverflow.com/questions/24119684  | 摸瓜V2引擎  |
| http://lame.sf.net  | lib/arm64-v8a/libavcodec.so  |
| http://www.twolame.org/  | lib/arm64-v8a/libavcodec.so  |
| http://ultravideo.cs.tut.fi/  | lib/arm64-v8a/libavcodec.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/arm64-v8a/libavformat.so  |
| http://%s:%d%s  | lib/arm64-v8a/libavformat.so  |
| http://%s%s  | lib/arm64-v8a/libavformat.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/arm64-v8a/libavformat.so  |
| https://github.com/flutter/flutter/issues/73620.  | lib/arm64-v8a/libflutter.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/arm64-v8a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/arm64-v8a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/arm64-v8a/libmobileffmpeg.so  |
| http://lame.sf.net  | lib/armeabi-v7a/libavcodec.so  |
| http://www.twolame.org/  | lib/armeabi-v7a/libavcodec.so  |
| http://ultravideo.cs.tut.fi/  | lib/armeabi-v7a/libavcodec.so  |
| http://lame.sf.net  | lib/armeabi-v7a/libavcodec\_neon.so  |
| http://www.twolame.org/  | lib/armeabi-v7a/libavcodec\_neon.so  |
| http://ultravideo.cs.tut.fi/  | lib/armeabi-v7a/libavcodec\_neon.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/armeabi-v7a/libavformat.so  |
| http://%s:%d%s  | lib/armeabi-v7a/libavformat.so  |
| http://%s%s  | lib/armeabi-v7a/libavformat.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/armeabi-v7a/libavformat.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/armeabi-v7a/libavformat\_neon.so  |
| http://%s:%d%s  | lib/armeabi-v7a/libavformat\_neon.so  |
| http://%s%s  | lib/armeabi-v7a/libavformat\_neon.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/armeabi-v7a/libavformat\_neon.so  |
| https://github.com/flutter/flutter/issues/73620.  | lib/armeabi-v7a/libflutter.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/armeabi-v7a/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libmobileffmpeg.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/armeabi-v7a/libmobileffmpeg\_armv7a\_neon.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/armeabi-v7a/libmobileffmpeg\_armv7a\_neon.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/armeabi-v7a/libmobileffmpeg\_armv7a\_neon.so  |
| http://lame.sf.net  | lib/x86/libavcodec.so  |
| http://www.twolame.org/  | lib/x86/libavcodec.so  |
| http://ultravideo.cs.tut.fi/  | lib/x86/libavcodec.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/x86/libavformat.so  |
| http://%s:%d%s  | lib/x86/libavformat.so  |
| http://%s%s  | lib/x86/libavformat.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/x86/libavformat.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/x86/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/x86/libmobileffmpeg.so  |
| http://lame.sf.net  | lib/x86\_64/libavcodec.so  |
| http://www.twolame.org/  | lib/x86\_64/libavcodec.so  |
| http://ultravideo.cs.tut.fi/  | lib/x86\_64/libavcodec.so  |
| http://dashif.org/guidelines/last-segment-number  | lib/x86\_64/libavformat.so  |
| http://%s:%d%s  | lib/x86\_64/libavformat.so  |
| http://%s%s  | lib/x86\_64/libavformat.so  |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd  | lib/x86\_64/libavformat.so  |
| https://github.com/flutter/flutter/issues/73620.  | lib/x86\_64/libflutter.so  |
| https://android.googlesource.com/toolchain/llvm-project  | lib/x86\_64/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe'  | lib/x86\_64/libmobileffmpeg.so  |
| http://www.ffmpeg.org/schema/ffprobe  | lib/x86\_64/libmobileffmpeg.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| twolame-discuss@lists.sourceforg  | lib/arm64-v8a/libavcodec.so  |
| appro@openssl.org  | lib/arm64-v8a/libflutter.so  |
| ffmpeg-devel@ffmpeg.org  | lib/arm64-v8a/libmobileffmpeg.so  |
| twolame-discuss@lists.sourceforg  | lib/armeabi-v7a/libavcodec.so  |
| twolame-discuss@lists.sourceforg  | lib/armeabi-v7a/libavcodec\_neon.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libmobileffmpeg.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libmobileffmpeg\_armv7a\_neon.so  |
| twolame-discuss@lists.sourceforg  | lib/x86/libavcodec.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86/libmobileffmpeg.so  |
| twolame-discuss@lists.sourceforg 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/x86\_64/libavcodec.so  |
| 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/x86\_64/libavformat.so  |
| ffmpeg-devel@ffmpeg.org  | lib/x86\_64/libmobileffmpeg.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: C=100000, ST=hangzhou, L=hangzhou, O=wp4665708, OU=wp4665708, CN=wp4665708 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-04 00:22:47+00:00 有效期至: 2079-02-05 00:22:47+00:00 发行人: C=100000, ST=hangzhou, L=hangzhou, O=wp4665708, OU=wp4665708, CN=wp4665708 序列号: 0x2bfdf98 哈希算法: sha256 md5值: c5b15ece0e3eb849230088599fcdaccf sha1值: e34fe09c51d5390eb28c0303567195a85b984beb sha256值: f4281816d1ddd4c82a3112651761750339a573bc4a57d54312e0880300c37311 sha512值: 0b3113192186324108fbf760c660ef52c377d5f7ff8d8f601c0d98f5f0351002a17fd74a43f00edc85b102c83b9dfe788df54ef131ff9e1a207779ed5f7e2c82**

## **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 |
| --- | --- | --- | --- |
|  | 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。**