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

**91茄子（ 4.0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 | 91茄子 |
| 版本 | 4.0 |
| 包名 | com.qnmd.a91qz.sj0eoe |
| 域名线索 | 25条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2024年9月19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 | qz-ovbh1qz.apk |
| 文件大小 | 10.91MB |
| MD5值 | 9a5b565a0cba3dbe0387a8a5b7fbf2b1 |
| SHA1值 | 76a97a1c475252a2f7bf8291a660bd00875a9911 |
| SHA256值 | 0f1dad385450cfdddd0f2aa122b76478c8a1c47b56cab47dafb3a5a61f603d87 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 91茄子 |
| 包名 | com.qnmd.a91qz.sj0eoe |
| 主活动Activity | com.qnmd.qz.ui.splash.SplashActivity |
| 安卓版本名称 | 4.0 |
| 安卓版本 | 6 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| loggw-exsdk.alipay.com | IP: 110.76.6.75 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| dashif.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| mcgw.alipay.com | IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang  |
| mobilegw.alipay.com | IP: 203.209.255.238 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-w3.kjds498.com | 没有服务器地理信息.  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息.  |
| schemas.android.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| m.alipay.com | IP: 203.209.245.120 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ns.adobe.com | 没有服务器地理信息.  |
| api-456.fdgasd632x.com | 没有服务器地理信息.  |
| api-01.dushnn.com | IP: 8.218.155.226 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| mobilegw.aaa.alipay.net | 没有服务器地理信息.  |
| playready.directtaps.net | IP: 104.45.231.79 所属国家: United States of America 地区: California 城市: San Francisco  |
| mclient.alipay.com | IP: 220.181.135.162 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  |
| api-qz.skpedj.com | IP: 104.21.28.86 所属国家: United States of America 地区: California 城市: San Francisco  |
| wappaygw.alipay.com | IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang  |
| mobilegw.stable.alipay.net | 没有服务器地理信息.  |
| h5.m.taobao.com | IP: 220.181.135.167 所属国家: China 地区: Beijing 城市: Beijing  |
| api-qz.shcinn.com | IP: 47.243.241.254 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Manchester  |
| api01.shejdf.com | IP: 8.218.30.161 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api-qa.gdfazqz65.com | IP: 8.218.30.161 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://h5.m.taobao.com/mlapp/olist.html  | f2/b.java  |
| https://mobilegw.alipay.com/mgw.htm  | f2/d.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | o0/g.java  |
| http://dashif.org/guidelines/last-segment-number  | n5/d.java  |
| http://127.0.0.1:  | m9/d.java  |
| https://mcgw.alipay.com/sdklog.do  | j2/a.java  |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do  | j2/a.java  |
| https://mobilegw.alipay.com/mgw.htm  | j2/a.java  |
| http://www.w3.org/ns/ttml  | y5/c.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/ShitTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/bumptech/glide/d.java  |
| http://m.alipay.com/?action=h5quit  | com/bumptech/glide/d.java  |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm?  | com/alipay/sdk/app/PayTask.java  |
| https://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://wappaygw.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/service/rest.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/home/exterfaceAssign.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| http://mclient.alipay.com/cashier/mobilepay.htm  | com/alipay/sdk/app/PayTask.java  |
| https://mobilegw.alipay.com/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.aaa.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw-1-64.test.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://mobilegw.stable.alipay.net/mgw.htm  | com/alipay/apmobilesecuritysdk/b/a.java  |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java  |
| http://api01.shejdf.com/qzapi/  | i8/o.java  |
| http://api-01.dushnn.com/qzapi/  | i8/o.java  |
| http://api-qz.shcinn.com/qzapi/  | i8/o.java  |
| http://api-qz.skpedj.com/qzapi/  | i8/o.java  |
| http://api-qa.gdfazqz65.com/qzapi/  | i8/o.java  |
| http://api-456.fdgasd632x.com/qzapi/  | i8/o.java  |
| http://api-w3.kjds498.com/qzapi/  | i8/o.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | db/d.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | db/f.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 5iqiezi@gmail.com  | m8/a.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13222222222  | u4/b.java  |
| 17179869184  | tv/danmaku/ijk/media/player/IjkMediaMeta.java  |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 签名算法: rsassa\_pkcs1v15 有效期自: 2023-08-29 20:00:01+00:00 有效期至: 2051-01-14 20:00:01+00:00 发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown 序列号: 0x756b85fc 哈希算法: sha256 md5值: 802836d64610f2eda40c49d871c28625 sha1值: d03f4d1bae91c8a0f211e7801b54dab43dd8f340 sha256值: 688308d871a153b6d5cb6aaa037b12d4f67fc266c22e0251b5ff32ac445b6bba sha512值: 1a3975d7d716b84dd631b151e03f397c6de28c678063d5025efd13805e83599e8c2b6682bc3f7ab40505be7b169e981e0b65174805e0a65625a825adb4344ae6 公钥算法: rsa 密钥长度: 2048 指纹: 8eda6cac92ab61b1ecc0291129b810ba23d41e4535eb33b29ed9a35b37864f8b**

## **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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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。 |

## **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。**