MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

会议服务 V1.0.2.2.APK

APP名称:	会议服务
包名:	com.itc.paperless.meetingservices.store
域名线索:	4条
URL线索:	6条
邮箱线索:	0条
分析日期:	2022年2月2日 20:12

文件信息

文件名: huiyifuwu563015.apk
文件大小: 4.03MB
MD5值: a69f0160f6e35fa3eb1d5ed904a1205a
SHA1值: 540af1765c6980ed5ead073afd889a01725d2197
SHA256值: dac1f30503903c2666609122b457c60a0cd3d2d02ee227e891f454e3d64de3cd

APP 信息

App名称: 会议服务
包名: com.itc.paperless.meetingservices.store
主活动**Activity:** com.itc.paperless.meetingservices.store.activity.LaunchAnimationActivity
安卓版本名称: V1.0.2.2
安卓版本: 3

域名线索

域名	是否危险域名	服务器信息
www.eclipse.org	good	**IP:** 198.41.30.198 **所属国家:** Canada **地区:** Ontario **城市:** Ottawa **纬度:** 45.345139 **经度:** -75.765076 **查看地图:** Google Map

域名	是否危险域名	服务器信息
netty.io	good	**IP:** 172.67.130.186 **所属国家:** United States of America **地区:** California **城市:** San Francisco **纬度:** 37.775700 **经度:** -122.395203 **查看地图:** Google Map
www.openssl.org	good	**IP:** 23.2.241.11 **所属国家:** United States of America **地区:** Texas **城市:** Dallas **纬度:** 32.783058 **经度:** -96.806671 **查看地图:** Google Map
wiki.eclipse.org	good	**IP:** 198.41.30.195 **所属国家:** Canada **地区:** Ontario **城市:** Ottawa **纬度:** 45.345139 **经度:** -75.765076 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java

URL信息	Url所在文件
https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
http://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
http://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html#alpn-starting	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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。
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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

向手机申请的权限	是否危险	类型	详细情况
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.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=paperless
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-12-03 02:41:45+00:00
Valid To: 2066-11-21 02:41:45+00:00
Issuer: CN=paperless
Serial Number: 0x3a3d42b5
Hash Algorithm: sha256
md5: e23b8160e77b1a5acedf0abdca5b2efe
sha1: 384d56dbd41475c2a99edc5826c0c9758cca29e3

sha256: aef56fe28494fb458468c1c593977981c38455f7d1c2ea6c8b4b8b6625bfd3b6
sha512: 99511f6a81d6fc17be2a515903209fdc7c5b5acc920eded522ba380239f68598c6ae551dafafb1b9465535c5a1de2f5ae84250e4f9b2b2ff8b6b078b841c8fec
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: ef0ea71ea786b421e7bb37058ea2bff705bab4c2f5e91da6414a6377fb7d8a0c

加壳分析

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>壳列表</th><th>详细情况</th></tr>
<tr><td>编译器</td><td>r8</td></tr>
</table>
</td></tr>
</table>
