MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

云办APP 1.0.18.APK

APP名称:	云办APP
包名:	com.meeting.recordcommon
域名线索:	1条
URL线索:	2条
邮箱线索:	0条
分析日期:	2022年2月3日 13:15

文件信息

文件名: yunban.apk
文件大小: 4.75MB
MD5值: 5569c41230720f60e249b1654a1af5fa
SHA1值: 7b73ecff140d0e5f5c93326a502852e0af7195c0
SHA256值: f7ef151359bc02c5c6e191e51f5df04c2d7d94ebf6a50ca0d5f57d6b6fab0d82

APP 信息

App名称: 云办APP
包名: com.meeting.recordcommon
主活动**Activity:** com.meeting.recordcommon.MainActivity
安卓版本名称: 1.0.18
安卓版本: 1

域名线索

域名	是否危险域名	服务器信息
mr1.someabc.net	good	**IP:** 8.133.173.133 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

URL线索

URL信息	Url所在文件
http://mr1.someabc.net/index.php?	com/meeting/recordcommon/config/ApiConfig.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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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.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: C=CN, ST=Minhang, L=Shanghai, O=Shuaidong, OU=Shuaidong, CN=George Wu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-03-31 01:58:56+00:00
Valid To: 2045-03-25 01:58:56+00:00
Issuer: C=CN, ST=Minhang, L=Shanghai, O=Shuaidong, OU=Shuaidong, CN=George Wu
Serial Number: 0x3b5e1dfd
Hash Algorithm: sha256
md5: 31852e29baecfaecbfb2b66dba052077
sha1: d9cdd4ad66b27b2048e52826b1b1479eb3bca421
sha256: 72039d6e0d40490b54727ce5f4f5337030c3fdb18aeeb3c741ab7ef9c4545b63
sha512: c528df8f64213f2f5231a6723f3566cd245ed78536454882f207a3f6e39716feca690d284ddaa984b72eb2faebac5e6be57e65d81084012f6b116fcb2e97efd7
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: b7f88b4ed279205555cfe2f2e44b2d4725861bdfb0b236613555899dfd5defda

加壳分析

文件列表	分析结果
classes.dex	<table><tr><th>壳列表</th><th>详细情况</th></tr><tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr></table>
