MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

协同管理 1.0.3.APK

APP名称:	协同管理
包名:	simu.mes
域名线索:	1条
URL线索:	3条
邮箱线索:	0条
分析日期:	2022年2月3日 12:44

文件信息

文件名: xietongguanli540604.apk
文件大小: 8.07MB
MD5值: 546d85675f73654f8227c4e3e7a6c221
SHA1值: 3aafc501768ab6792a54d0ab70a1e86d91c6f976
SHA256值: 3fc13aa219e48b13515ad6defd50c984714ee8f6d601c51c8de3672104fb77f9

APP 信息

App名称: 协同管理
包名: simu.mes
主活动**Activity:** simu.mes.MainActivity
安卓版本名称: 1.0.3
安卓版本: 10003

域名线索

域名	是否危险域名	服务器信息
182.92.20.189	good	**IP:** 182.92.20.189 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://182.92.20.189:9099/	cn/jiguang/a/a/c/h.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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
simu.mes.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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

向手机申请的权限	是否危险	类型	详细情况
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
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

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=US, O=Android, CN=Android Debug
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2015-04-21 07:30:57+00:00
Valid To: 2045-04-13 07:30:57+00:00
Issuer: C=US, O=Android, CN=Android Debug
Serial Number: 0x6e5147ca
Hash Algorithm: sha256
md5: ac21580cbe6d153d3985942d4edaaaa7
sha1: 33921f55c5b5ee2db6ada62c5f864044a3df2098

sha256: 8e6379cffd9259374aaa34e1dd3e0cf340e655a1789a3a174c02c827c1b2a227
sha512: 24a1a7a3f410c0ac03fdce798102f00e8e3ef87df60160896f66fd4f518d5ce40e239d09966548d447bc67e9f91bff53b6e8342194d6dbf6a5e4f167c116a359
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: c6cf686efa56842d4eee3bc413a87071d783b4e1d26be4b0b339df858419d529

Exodus威胁情报

名称	分类	URL链接
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343

加壳分析

文件列表	分析结果

文件列表	分析结果
classes.dex	

壳列表	详细情况
反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check possible Build.SERIAL check network operator name check device ID check subscriber ID check
反调试	Debug.isDebuggerConnected() check
编译器	dx (possible dexmerge)
Manipulator Found	dexmerge
