

APP线索分析报告

报告由模瓜APP分析平台(mogua.co) 生成



₩ Interval Timer 1.2.APK

APP名称: Interval Timer

包名: com.artiomapps.timerworkout

域名线索: 1条

URL线索: 1条

邮箱线索: 1条

分析日期: 2022年1月20日 21:57

文件名: jsfzjsq536545.apk

文件大小: 4.96MB

MD5值: badc8d8a025703c837fcea12cd832dd3

SHA1值: f929f99c4fda7f2c3b824b5f54c1467359276d1b

SHA256值: a2c1eece6d037ac6a07a3c07484b57eabd70b865cc40f88773b547536d142da3

i APP 信息

App名称: Interval Timer

包名: com.artiomapps.timerworkout

主活动**Activity:** com.artiomapps.timerworkout.SplashActivity

安卓版本名称: 1.2 安卓版本: 3

Q 域名线索

域名	是否危险域名	服务器信息
artiomapps.com	good	IP: 172.67.213.191 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map



URL信息	Url所在文件
http://artiomapps.com/privacypolicy.html	Android String Resource

✓邮箱线索

邮箱地址	所在文件
simple.willgood@gmail.com	Android String Resource

₩ 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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_NOTIFICATION_POLICY	正常		希望访问通知策略的应用程序的标记权限。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字

向手机申请的权限	是否 危险	类型	详细情况
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.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



APK is signed

v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates Subject: CN=Artiom Apps

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2019-02-09 11:30:12+00:00 Valid To: 2044-02-03 11:30:12+00:00

Issuer: CN=Artiom Apps Serial Number: 0x34bb1426 Hash Algorithm: sha256

md5: 70f65bd2d4c30c371612d41fa8a70dae

sha1: ce81cd337df02236de99612249914447a94187ff

sha256: b3f19efd7c81fb490fb41353dd9a54ea8bbb85532b55aba343f5f7fdbeacc329

sha512: c5e1392319317d7979bf356ea076b779f3469879f42d42fae259b105dd2bc8f1782febcf42bd99fd0cca6f1c027ec84ca1c3284ebce75879809d22da38f7cf42

PublicKey Algorithm: rsa

Bit Size: 2048

Fingerprint: ea6ead317ccf40741ee737b52ae7538726ec605bdf706c1fa46742d55c4937d9



名称	分类	URL链接
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

命加壳分析

文件列表	分析结果				
classes2.dex	売列表	详细情况			
Classesz.dex	编译器	r8 without marker (suspicious)			
	売列表	详细情况			
	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check possible VM check			
	编译器	r8			

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析