

APP线索分析报告

报告由模瓜APP分析平台(mogua.co)生成



♦ Vbitex 0.0.9.APK

APP名称: Vbitex

包名: com.h56497825.uqb

域名线索: 6条

URL线索: 9条

邮箱线索: 1条

分析日期: 2022年1月20日 22:17

文件名: vbitex.apk 文件大小: 4.58MB

MD5值: 69e1bfc296c132581890f1e962e5edf2

SHA1值: 0ebe90e25f4d6daafd1ee25f0ab5009f9c341abb

\$HA256值: 37e3d243cc8676ef3cc3c29ff4170bc51b32e06b2f3516c617df7df61f611ec6

i APP 信息

App名称: Vbitex

包名: com.h56497825.uqb

主活动**Activity:** com.uzmap.pkg.EntranceActivity

安卓版本名称: 0.0.9

安卓版本: 9

0 域名线索

域名	是否危险域名	服务器信息
s.apicloud.com	good	没有服务器地理信息.
p.apicloud.com	good	IP: 47.93.154.30 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
as.apicloud.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
a.apicloud.com	good	IP: 182.92.145.58 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
d.apicloud.com	good	IP: 47.94.176.24 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
r.apicloud.com	good	IP: 182.92.145.58 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
https://a.apicloud.com	compile/Properties.java

URL信息	Url所在文件
https://d.apicloud.com	compile/Properties.java
https://s.apicloud.com	compile/Properties.java
https://p.apicloud.com	compile/Properties.java
https://r.apicloud.com	compile/Properties.java
https://as.apicloud.com	compile/Properties.java

✓邮箱线索

邮箱地址	所在文件
developer@apicloud.com	com/uzmap/pkg/uzcore/b/d.java

缸此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

向手机申请的权限	是否危险	类型	详细情况
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上 显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
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_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置(如果可用)。 恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
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



APK is signed v1 signature: True v2 signature: True v3 signature: False

Found 1 unique certificates

Subject: C=(zh), ST=(Beijing), L=(Beijing), O=(56497825@qq.com), OU=(56497825@qq.com), CN=(j56497825)

Signature Algorithm: rsassa_pkcs1v15 Valid From: 2018-12-15 02:15:12+00:00 Valid To: 2118-11-21 02:15:12+00:00

Issuer: C=(zh), ST=(Beijing), L=(Beijing), O=(56497825@qq.com), OU=(56497825@qq.com), CN=(j56497825)

Serial Number: 0x41d2ce48 Hash Algorithm: sha256

md5: b13b9396b38848dde2daf51417df3db9

sha1: 1b972532f14a59e55b3c8efb61cf06a26de64e2f

sha256; 7c7e71237586ae82c538a95209008e2558e10bdaaf99aea94fbe2287196eabd5

sha512: 44dd79af40e41990a82fab5cc2442768b240e2786db31b976b83a834b34df400805ed37f6ea397ccfbc75481285663a7f00599bc41e8b16a964f7489740c1c0c

PublicKey Algorithm: rsa

Bit Size: 1024

Fingerprint: 666f309799aea4e8927cf899c53e8e88aa776a00f77546ec8c00aeb739f732a0

命加壳分析

文件列表	分析结果				
	売列表				
classes.dex	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check possible Build.SERIAL check			
	编译器	dx			

报告由 摸瓜平台 自动生成,并非包含所有检测结果,有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析