MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

应用商店 3.8.7.APK

APP名称:	应用商店
包名:	com.sony.appstore
域名线索:	13条
URL线索:	11条
邮箱线索:	0条
分析日期:	2022年1月26日 20:14

文件信息

文件名: ssyyb.apk
文件大小: 2.94MB
MD5值: a0c0aa8c3afd2922206a7fd8596f7792
SHA1值: 4a7578e07f66959d740f0084f6668811402abbd8
SHA256值: 981eab61302448328f8a2566eb8604666d1856f024677fda957bd3c73e8b223f

APP 信息

App名称: 应用商店
包名: com.sony.appstore
主活动**Activity:** com.tencent.appstore.splash.LogoActivity
安卓版本名称: 3.8.7
安卓版本: 20180828

域名线索

域名	是否危险域名	服务器信息
static.kf0309.3g.qq.com	good	**IP:** 101.89.39.96 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061 查看地图: Google Map

域名	是否危险域名	服务器信息
android.rqd.qq.com	good	IP: 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
oth.eve.mdt.qq.com	good	IP: 175.27.0.70 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
183.36.108.226	good	IP: 183.36.108.226 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
strategy.beacon.qq.com	good	IP: 121.51.80.238 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
oth.str.mdt.qq.com	good	IP: 183.36.108.32 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
cms.gtimg.com	good	IP: 182.254.54.224 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
qzs.qq.com	good	IP: 182.254.48.158 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
monitor.uu.qq.com	good	IP: 182.254.88.185 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

域名	是否危险域名	服务器信息
www.openssl.org	good	IP: 104.111.199.231 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692 查看地图: Google Map
rqd.uu.qq.com	good	IP: 182.254.88.184 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map
android.bugly.qq.com	good	IP: 109.244.244.35 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
maweb.3g.qq.com	good	IP: 182.254.63.77 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298 查看地图: Google Map

URL线索

URL信息	Url所在文件
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://monitor.uu.qq.com/analytics/rqdsync	com/tencent/b/a/b.java
http://android.rqd.qq.com/analytics/async	com/tencent/b/a/b.java
http://maweb.3g.qq.com/welcome.html	com/tencent/basemodule/network/f.java
http://seatimg?params=	com/tencent/basemodule/d/c.java
http://static.kf0309.3g.qq.com/open/yyb/yunos_gift/gift.html	com/tencent/appstore/appdetail/view/GameDetailGiftCard.java
http://oth.eve.mdt.qq.com:8080/analytics/upload	com/tencent/beacon/a/a.java
http://oth.str.mdt.qq.com:8080/analytics/upload	com/tencent/beacon/a/a.java
http://183.36.108.226:8080/analytics/upload	com/tencent/beacon/a/a.java
http://oth.str.mdt.qq.com:8080/analytics/upload	com/tencent/beacon/a/e/a.java
http://oth.eve.mdt.qq.com:8080/analytics/upload	com/tencent/beacon/a/e/a.java
http://strategy.beacon.qq.com/analytics/upload	com/tencent/beacon/a/f/h.java
http://cms.gtimg.com/android_cms/goodnewapp/4a395c5e289a0f23c902157808f5587f.jpg	Android String Resource

URL信息	Url所在文件
http://qzs.qq.com/open/yyb/yunos_terms/index.html	Android String Resource
http://www.openssl.org/support/faq.html	lib/armeabi/libyyb_csech.so

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.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.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
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.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

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
com.android.alarm.permission.SET_ALARM	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.EXPAND_STATUS_BAR	正常	展开/折叠状态栏	允许应用程序展开或折叠状态栏
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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
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

向手机申请的权限	是否危险	类型	详细情况
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
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.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.DELETE_PACKAGES	系统需要	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

签名证书

APK is signed
v1 signature: True

v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=Beijing City, L=Beijing City, O=QZone Team of Tencent Company, OU=Tencent Company, CN=Android QZone Team
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2010-06-27 04:08:02+00:00
Valid To: 2035-06-21 04:08:02+00:00
Issuer: C=86, ST=Beijing City, L=Beijing City, O=QZone Team of Tencent Company, OU=Tencent Company, CN=Android QZone Team
Serial Number: 0x4c26cea2
Hash Algorithm: sha1
md5: a095641b30785f28642708f481603e0b
sha1: 2677c0f3bc06b2bb627c5653040e6da8b2f5e39c
sha256: 9c286b8beb45a6bc2642e2e52255c7f892573a7d5da7cb4598c419a46e898d36
sha512: 04008877a9efe8ac3eeaa59a002fa9f86d01a21a338c63e3282087bddc2f6d7293bd80da3becd7fd8b186fcb2d5ff9ca0d6c4c8b9f8694ac362d2a9b36cbce95

Exodus威胁情报

名称	分类	URL链接
Bugly		https://reports.exodus-privacy.eu.org/trackers/190

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.tencent.appstore.activity.AppLinkActivity	Schemes: toasp://, Hosts: appstore,

加壳分析

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.MANUFACTURER check Build.HARDWARE check Build.TAGS check device ID check subscriber ID check possible ro.secure check emulator file check 编译器: dx

---