# 对 CarrierIQ 木马的综合分析报告

安天实验室

2011.11

## 目录

# 一、事件概述

## 1. 背景

近日，Android 开发者 Trevor Eckhart 发现 Carrier IQ 公司与移动运营商合作预装入手机系统中的软件存在严重的隐私搜集行为[1] 。

该公司的官方介绍称[2] ：

*“Carrier IQ 是移动服务智能解决方案的市场领导者，为移动运营商和设备制造商搜集和管理终端用户信息的途径做出了革命性的突破。”*

美国移动运营商 Sprint 的发言人 Jason Gertzen 在邮件中称：

*“它（Carrier IQ 公司的产品）搜集足够的信息，从而了解我们网络中移动设备的用户体验，并为使用和网络连接的问题提出解决方案。我们没有、也无法通过这一工具查看用户的短信内容、照片、视频等。”*

然而，根据该公司公开的产品专利和产品培训资料，该产品搜集与网络相关的信息，包括语音和数据服务；还搜集与网络无关的信息，包括设备类型、可用内存和电池电量、设备中软件的类型、设备的地理位置信息、设备用户的按键信息、设备的使用历史等。这些信息被传回至 Carrier IQ 公司的服务器进行统计分析。其提供的后台产品可以根据 IMEI 或 IMSI 对任何一个设备进行详细的历史记录查询，即用户的隐私被完全暴露给该公司及其产品用户。

运营商 Verizon 和 Sprint 在其多款手机中预装了这一软件，涉及 Android、Symbian 和 BlackBerry 三个平台。相关报道称受影响设备数量达 1.41 亿[4] 。多个著名的第三方定制 ROM 提供商，例如 CyanogenMod，也曾采用这一软件。

事件曝光后，Carrier IQ 公司向 Trevor Eckhart 送抵了措辞强烈的侵略性停止和终止函，称其使用和备份该公司培训资料构成侵权。有律师指出 Eckhart 的行为受到美国著作权法豁免保护。11 月 24 日，Carrier IQ 公司撤销控诉，并再次强调其软件“*并不监视用户数据，记录键击，或提供跟踪信息，只是识别掉线，电池问题，并且预测移动网络可能出现的问题，同时帮助运营商使顾客服务更有效。*”[5]

## 2. 本报告概述

安天实验室对上述事件及其相关样本进行了深入分析。主要结论包括：

- ✓ 在 Sprint 公司官方 ROM 中、多个第三方定制 ROM 中发现该样本

- ✓ 有国内用户的手机上含有该样本
- ✓ 样本由多个预装入 ROM 的模块组成
- ✓ 样本搜集当前移动运营网络相关信息
- ✓ 样本中包含搜集预装入手机的多个软件隐私信息的代码
- ✓ 样本中包含将搜集到的隐私信息回传至指定服务器的代码
- ✓ 样本运行后，将开启一个本地服务
- ✓ 样本运行后，能触发调用回传代码的本地行为
- ✓ 当样本收到特定格式的短信内容或 WAP 推送内容后，会将搜集到的隐私信息回传至服务器
- ✓ 该样本存在 Android、Symbian、BlackBerry 三个平台的试用版软件
- ✓ 该样本比其试用版软件在用户行为表现上具有更高的隐蔽性
- ✓ CarrierIQ 公司的产品培训资料可以从另一个角度说明其产品搜集用户隐私
- ✓ CarrireIQ 公司提供的后台服务支持对指定手机和用户的单独查询，并能获取所有回传隐私的详细数据

# 二、样本传播渠道

在 Carrier IQ 公司的培训资料中，有该软件在 Android、Symbian S60、BlackBerry 4.7.0 三个平台的试用版本。其中，就 Android 系统，目前已知以下刷机 ROM 中存在该软件（图 1）：

- Sprint 公司为 HTC G3 Hero 手机提供的官方 ROM
- Sprint 公司为 HTC EVO 3D Shooter 手机提供的官方 ROM
- OMJ 为 HTC EVO 4G 手机定制的 Android 2.2 第三方 ROM
- Villain 为 HTC G3 Hero 手机定制的第三方 ROM，5.4 和 5.5 版
- Synergy 为 HTC EVO, INCredible, MyTouch 4G 手机定制的第三方 ROM

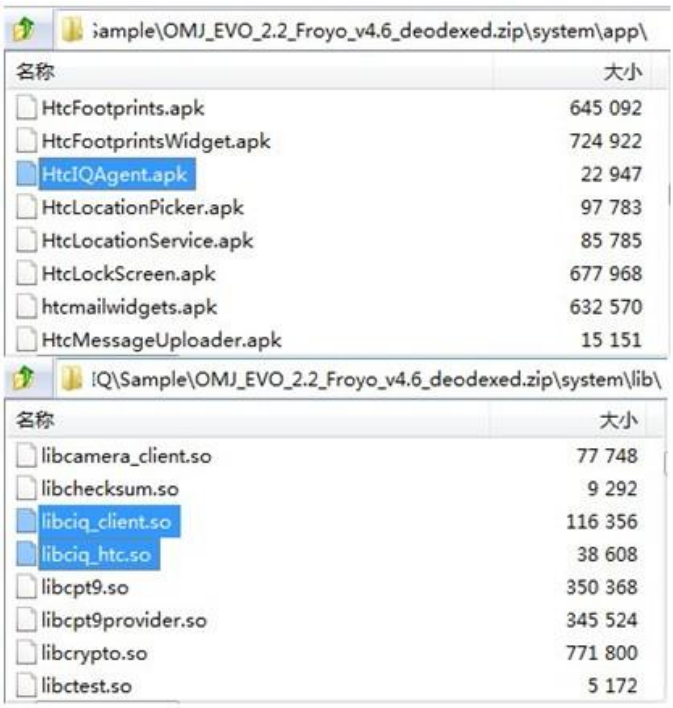



**图 1　在刷机 ROM 中发现该软件**

此外，从今年下半年开始，国外多个第三方定制 ROM 提供商开始有计划地从提供的所有 ROM 中移除 Carrier IQ 软件相关的组件。目前在部分 ROM 中还可以看到一些没有彻底清理干净的残留组件（图 2）。

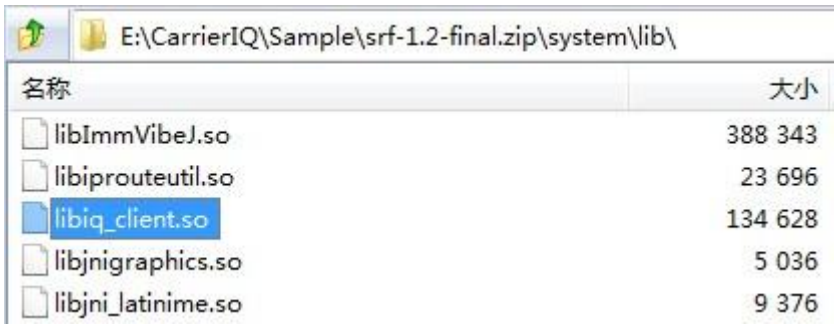



**图 2　第三方 ROM 中残留的软件组件**

上述官方 ROM 和第三方 ROM 绝大部分为国外运营商或定制商提供，其中一般不含中文资源。但是从搜索结果来看，有一部分国内用户的手机中确实存在这个软件，并且在手机中长期运行（图 3）。

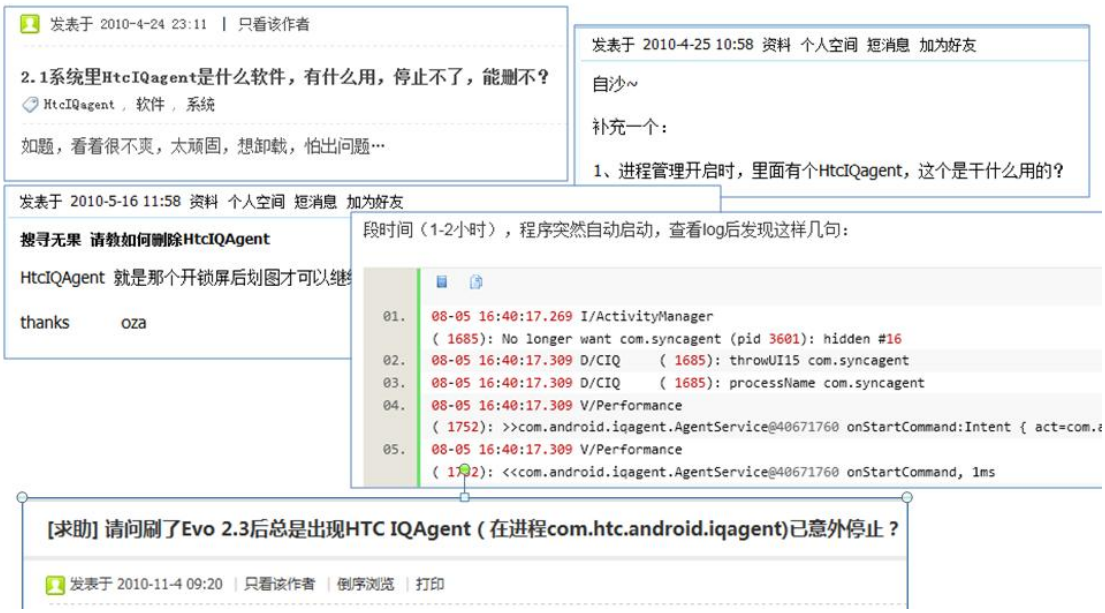



**图 3　国内用户的手机中存在该软件**

# 三、样本静态分析

## 1. 样本的模块组成

在为 HTC 手机提供的 Android ROM 中，该软件由以下文件组成：

- /system/app/HtcIQAgent.apk
- /system/app/HtcIQAgent.odex
- /system/app/IQRD.apk
- /system/app/IQRD.odex
- /system/lib/libhtciqagent.so
- /system/lib/libciq_htc.so
- /system/lib/libciq_client.so
- /system/etc/iqprofile.pro
- /system/bin/iqfd
- /system/bin/iqd

其中包含两个 APK 安装文件，三个 SO 动态链接库，两个 ELF 可执行文件，以及一个配置文件 iqprofile.pro。这些文件分布在 ROM 中四个不同的目录下。下面对这些文件逐一分析。

## 2. APK 安装文件

### 1) IQRD.apk

IQRD.apk 由一个服务 com.htc.android.iqrd.IqService，一个接收器 com.htc.android.iqrd.StateReceiver 和一个活动 com.htc.android.iqrd.IqActivity 组成，没有启动菜单图标。在运行时，其还会注册两个接收器（图 4），其中一个接收器的触发行为包括：

- com.android.phone.HtcCdmaPhoneApp.WAKE_CIQ
- com.android.internal.policy.impl.SHUTDOWN_CIQ
- com.android.phone.HtcCdmaPhoneApp.DISABLE_CIQ
- com.android.phone.HtcCdmaPhoneApp.NAI_INFO

另一个的触发行为为：

- com.android.phone.MESSAGE_SENT

目前仍不知道这些行为由哪个程序触发。

```
IntentFilter localIntentFilter1 = new IntentFilter("com.android.phone.HtcCdmaPhoneApp.WAKE_CIQ");
localIntentFilter1.addAction("com.android.internal.policy.impl.SHUTDOWN_CIQ");
localIntentFilter1.addAction("com.android.phone.HtcCdmaPhoneApp.DISABLE_CIQ");
localIntentFilter1.addAction("com.android.phone.HtcCdmaPhoneApp.NAI_INFO");
Context localContext2 = this.mContext;
BroadcastReceiver localBroadcastReceiver1 = this.mFDReceiver;
Handler localHandler1 = this.mHandler;
Intent localIntent1 = localContext2.registerReceiver(localBroadcastReceiver1, localIntentFilter1,
```

**图 4　IQRD.apk 注册接收器**

IQRD.apk 需要的额外权限如下：

- CALL_PHONE：允许应用程序在您不介入的情况下拨打电话。
- READ_PHONE_STATE：允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
- SEND_SMS：允许应用程序发送短信。
- CHANGE_NETWORK_STATE：允许应用程序更改网络连接的状态。

IQRD.apk 使用了一个特殊的属性：android:sharedUserId="android.uid.phone"，设置该属性要求其与系统中负责通话的应用程序 Phone.apk 具有相同的签名。设置了该属性后，IQRD.apk 与 Phone.apk 将以相同的 UID 运行，因此双方的数据可以完全为对方获得。

在该样本的 CDMA 版本中，会读取网络的 ESN、MEID、MDN、MSID、PRL、SPN、MIP、NAI 等信息，包括 NAI 的用户名和密码（图 5）。对 GDM 网络，则读取其网络相应的信息，如 MCC、MNC、APN 等。

```
public void readNAIPasswd(int paramInt)
{
  StringBuilder localStringBuilder1 = new StringBuilder();
  String str1 = NV_READ_ITEM_NAI_PASSWD;
  StringBuilder localStringBuilder2 = localStringBuilder1.append(str1);
  String str2 = String.valueOf(paramInt);
  String str3 = str2;
  if (paramInt == 0)
  {
    Message localMessage1 = this.mHandler.obtainMessage(14);
    mPhone.requestHtcDMCommand(str3, localMessage1);
    return;
  }
  if (paramInt != 1)
    return;
  Message localMessage2 = this.mHandler.obtainMessage(15);
  mPhone.requestHtcDMCommand(str3, localMessage2);
}
```

**图 5　IQRD.apk 读取 NAI 密码**

### 2)　HtcIQAgent.apk

该样本只有一个服务 com.htc.android.iqagent.AgentService，其触发条件包括 25 个类似于 com.htc.android.iqagent.action.ss1c 的行为。这些行为实际上与手机中预装的软件关联。

进一步分析代码可以看到，Carrier IQ 将这些触发行为的对象称之为 metric，这与其官方培训资料和专利中的命名是一致的。具体而言，该样本为系统预装的多款软件设置一个整数用于标识（图 6），再使用 byteToHexString 函数和 hexStringToByte 将这些整数与一个 metric 进行对应，从而将类似于 com.htc.android.iqagent.action.ss1c 的服务触发行为关联到不同的软件。

```
if (paramString.equals("com.telenav.app.android"))
{
  i = 12;
  continue;
}
if (paramString.equals("com.htc.soundrecorder"))
{
  i = 7;
  continue;
}
if (paramString.equals("com.android.vending"))
{
  i = 1;
  continue;
}
if ((paramString.equals("com.htc.android.omadm")) ||
{
  i = 24;
```

**图 6　HtcIQAgent.apk 为大量预装软件设置映射关系**

该样本中关联的预装软件包括：

- com.htc.android.htcime
- com.android.phone
- com.htc.calendar、com.android.calendar
- com.telenav.app.android
- com.htc.soundrecorder
- com.android.vending
- com.htc.android.omadm、com.smithmicro.DM
- com.htc.android.mail
- com.android.browser
- com.android.calculator2
- com.android.calculator
- com.google.android.youtube
- com.htc.pdfreader
- com.htc.music
- com.google.android.gm
- com.android.ft
- com.android.googleserarch
- com.android.mms
- com.android.launcher
- com.android.packageinstalller
- com.android.settings
- com.android.updater
- com.google.android.apps.gtalkservice
- com.google.android.apps.maps
- com.google.android.talk
- com.htc.streamplayer
- com.android.camera

- com.google.android.googleappps
- com.htc.dcs
- com.htc.album
- com.amazon.mp3
- com.handson.h2o.nfl
- com.handson.h2o.nascar09
- com.mobitv.client.sprinttv
- com.htc.android.teeter
- com.telenav.app.android.sprint

根据触发服务的不同行为，该样本经过上述对应得到行为对应的应用程序，进一步搜集相应的隐私信息，例如具体的 GPS 地理位置信息等（图 7）。

进一步地，当 HtcIQAgent.apk 搜集到这些信息后，调用本地 htciqagent.so 库文件提供的相应 JNI 接口，将这些隐私数据向服务器提交。

```
Intent localIntent11 = localIntent1;
String str28 = "GPSRequestType";
int i14 = 0;
short s12 = localIntent11.getShortExtra(str28, i14);
Intent localIntent12 = localIntent1;
String str29 = "GPSSource";
int i15 = 0;
short s13 = localIntent12.getShortExtra(str29, i15);
Intent localIntent13 = localIntent1;
String str30 = "GPSResult";
int i16 = 0;
short s14 = localIntent13.getShortExtra(str30, i16);
Intent localIntent14 = localIntent1;
String str31 = "GPSFieldsValid";
int i17 = 0;
short s15 = localIntent14.getShortExtra(str31, i17);
Intent localIntent15 = localIntent1;
String str32 = "Latitude";
long l9 = 65535L;
long l10 = localIntent15.getLongExtra(str32, l9);
Intent localIntent16 = localIntent1;
String str33 = "Longitude";
```

**图 7　HtcIQAgent.apk 搜集 GPS 信息**

## 3.　SO 动态链接库文件

HtcIQAgent.apk 调用了 htciqagent.so 提供的 JNI 接口。后者实际上也只是一个封装层，它包含两类函数（图 8），一类形如 Java_com_htc_android_iqagent_Controller_submitAL16，

是提供给 APK 的 JNI 接口，这些函数会调用内部实现的形如 actionAL16 的函数。APK 获得的隐私数据数量不同，这些 action 函数分别获取这些数据，将其拼接在一起，最后调用 IQ_SubmitMetric 来提交这些数据，并将信息来源类型作为参数传给它。


**图 8　htciqagent.so 中的部分函数**

IQ_SubmitMetric 实现于 libciq_client.so 中。它首先调用 iq_metric_might_be_interesting 函数判断是否感兴趣的数据，如果是，获取当前时间戳，然后调用 iq_submit_metric 提交数据。

## 4. 配置文件

文件 iqprofile.pro 被预装入 ROM 的/system/etc 目录。该文件被加密，但其中包含一个部分明文的 URL 如下：

https://collector.iota.spcsdns.net:10003/collector/c

其子域名 collector 的含义为“搜集者”。

iqprofile.pro 被 iqd 这个可执行文件调用。

## 5. ELF 可执行文件

在可执行文件 iqd 中，包含以下 URL：

http://collector.sky.carrieriq.com:7001/collector/c?cm_sl=5

# 四、样本动态分析

在包含样本的手机中,“所有应用程序”列表里包含名为 HTC IQAgent 和 IQRD 的程序（图 9）。其中，IQRD 需要的权限如图 10 所示。

需要指出的是，预装入 ROM 的 IQRD 所需权限比其在 AndroidManifest.xml 中要多，多出的部分包括：

- 允许读取和改写联系人信息
- 编辑、读取、接收短信与彩信
- 根据网络获取粗略的地理位置
- 创建蓝牙连接，Internet 访问
- 改变声音设置
- 蓝牙管理、改变 Wi-Fi 状态、改变 UI 设置、修改系统全局设置、设置时区、修改 APN 设置

这些权限超出了其在 AndroidManifest.xml 中申明的权限，是因为该程序使用了共享 UID：android.uid.phone，从而可以使用系统程序 com.android.phone 中的权限。

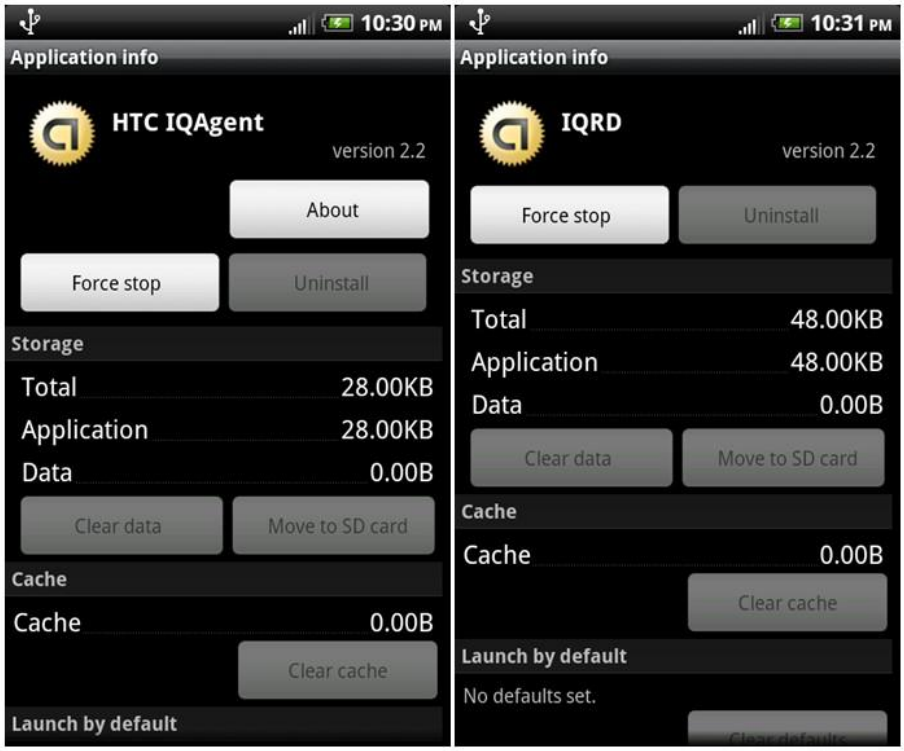



**图 9　样本对应的应用程序**

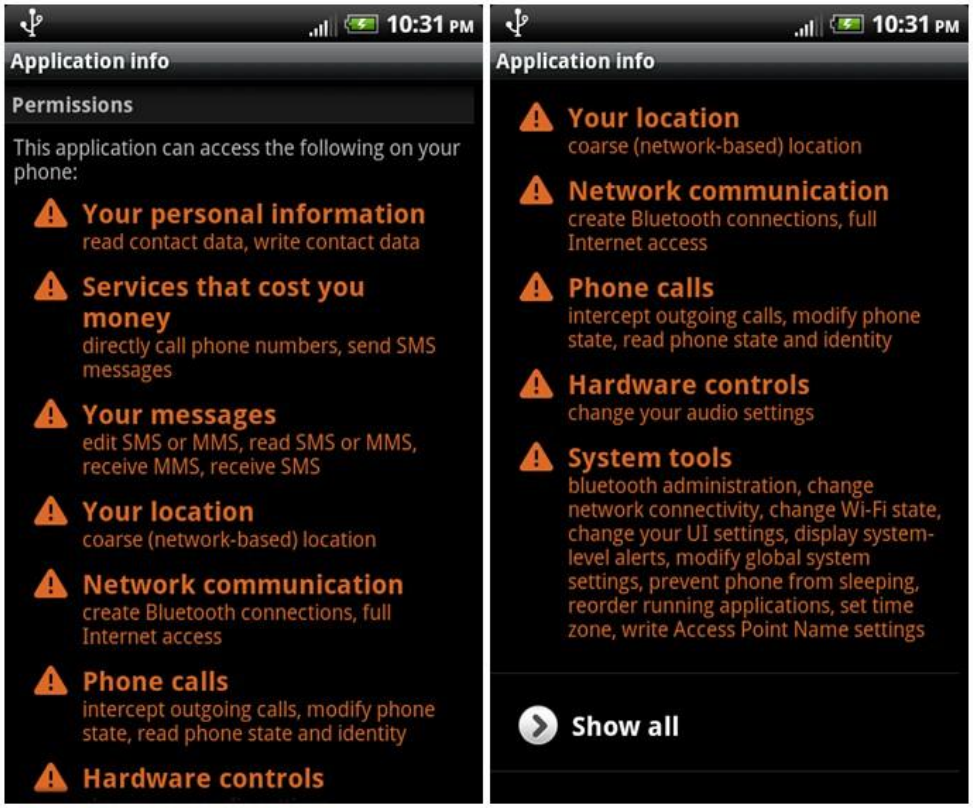



**图 10　IQRD 所需权限**

样本会启动服务 AgentService（图 11）。

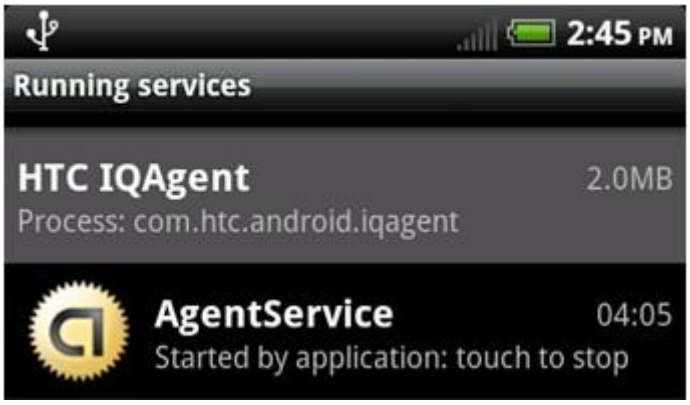



**图 11　HtcIQAgent 开启的服务**

当用户访问互联网网页，或者启动 Google 搜索时，该样本将输出调试信息（图 12）。这些调试信息是 htciqagent.so 文件中没有清理干净的调试代码输出的，位于其 JNI 接口 Java_com_htc_android_iqagent_Controller_submitAL15 的实现里（图 13）。而该 JNI 接口是在 HtcIQAgent.apk 搜集了与 Web 访问相关的隐私数据后调用的。

但是在整个样本运行期间，没有捕获到与回传隐私行为相关的网络数据。

| Application | Tag | Text |
| --- | --- | --- |
| com.htc.android.iqagent | dalvikvm | No JNI_OnLoa |
| com.htc.android.iqagent | dalvikvm | JNI WARNING: |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | dalvikvm | GC_EXPLICIT |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |
| com.htc.android.iqagent | com_htc_android_iqagent_Controller | submitAL15 |

**图 12　IQAgent 输出的调试信息**

```
 EXPORT Java_com_htc_android_iqagent_Controller_submitAL15
droid_iqagent_Controller_submitAL15
 PUSH.W          {R4-R8,LR}
 LDR             R4, =0x1918
 MOV             R7, R2
 ADR             R5, loc_17D0
 LDR             R1, =(aCom_htc_androi - 0x30E8)

                         ; DATA XREF: Java_com_htc_android_iqagent_
 ADDS            R3, R4, R5
 LDR             R2, =(aSubmital15 - 0x30E8)
 MOV             R4, R0
 ADDS            R1, R3, R1 ; "com_htc_android_iqagent_Controller"
 MOVS            R0, #4
 ADDS            R2, R3, R2 ; "submitAL15"
 BLX             __android_log_print
 LDR             R0, [R4]
```

**图 13　htciqagent.so 中残留的调试代码**

# 五、试用版软件分析

在 Carrier IQ 公司的培训资料中，有该软件在 Android、Symbian、BlackBerry 三个平台的试用版本：

- 用于 Android 系统的 IQAgent.apk
- 用于 Symbian S60 系统的 IQ_AgentVM_S603rdMRd.sisx
- 用于 BlackBerry 4.7.0 系统的 IQAgent.cod 等

需要特别强调的是，目前网络上已有的对该样本的分析[1] ，主要是对该试用版软件的分析，虽然它与真正装入到 ROM 的软件在代码上有非常多相似之处，但在表现给用户的行为上有较大差异。这一点将会在后面详细说明。

下面是对其 Android 版本的分析。

## 1. 静态分析

该样本需要较多的运行权限，包括：

- INTERNET：允许应用程序创建网络套接字。
- READ_PHONE_STATE：允许应用程序访问设备的手机功能。有此权限的应用程序可确定此手机的号码和序列号，是否正在通话，以及对方的号码等。
- RECEIVE_BOOT_COMPLETED：允许应用程序在系统完成启动后即自行启动。
- RECEIVE_SMS：允许应用程序接收和处理短信。
- MODIFY_PHONE_STATE：允许应用程序控制设备的电话功能。拥有此权限的应用程序可自行切换网络、打开和关闭无线通信等，而不会通知您。
- CHANGE_NETWORK_STATE：允许应用程序更改网络连接的状态。
- GET_TASKS：允许应用程序检索有关当前和最近运行的任务的信息。恶意应用程序可借此发现有关其他应用程序的保密信息。
- ACCESS_NETWORK_STATE：允许应用程序查看所有网络的状态。
- ACCESS_COARSE_LOCATION：访问粗略的位置源以确定手机的大体位置。
- ACCESS_FINE_LOCATION：访问精准的位置源，例如手机上的全球定位系统。
- ACCESS_WIFI_STATE：允许应用程序查看有关 Wi-Fi 状态的信息。
- READ_LOGS：允许应用程序从系统的各个日志文件中读取信息。这样，应用程序就可以发现关于您手机使用情况的一般信息，其中可能包含个人信息或私密信息。

- RECEIVE_WAP_PUSH：允许应用程序接收和处理 WAP 信息。
- PERSISTENT_ACTIVITY：允许应用程序部分持续运行，这样系统便不能将其用于其他应用程序。
- PROCESS_OUTGOING_CALLS：允许应用程序处理外拨电话或更改要拨打的号码。恶意应用程序可能会借此监视、另行转接甚至阻止外拨电话。
- WAKE_LOCK：允许应用程序防止手机进入休眠状态。
- BATTERY_STATS：允许修改收集的电池使用情况统计信息。普通应用程序不能使用此权限。

当手机的屏幕开启或关闭、系统启动完成、电池状态改变等时，将触发其接收器 com.carrieriq.trial.service.receivers.BootCompletedReceiver，该接受器启动服务 com.carrieriq.trial.service.IQService。

IQService 根据系统版本，调用释放的两个本地库文件 libiq_service_trial_1.6.so、libiq_service_trial_2.2.so 之一。


**图 14　libiq_service_trial_2.2.so 中实现了 HTTP 上传**

该样本检测拨出的电话，当发现号码为“#*47234#”时，禁止这次呼叫。该号码是移动运营商的 USSD 代码。

```
public void onReceive(Context paramContext,
{
  String str = paramIntent.getStringExtra("
  if (str == null)
    return;
  if (!str.equals("#*47234#"))
    return;
  abortBroadcast();
```

**图 15　IQAgent.apk 禁止拨打特定电话号码**

此外，该样本在运行后创建两个接收器，分别接收 android.provider.Telephony.SMS_RECEIVED 和 android.provider.Telephony.WAP_PUSH_RECEIVED 广播，在接收到短信或 WAP 推送信息后，取出其内容，调用 checkSMS 和 checkWAPPush 方法进行检查。如果是特定的内容，

则不显示该信息。

```
localIntentFilter1.addAction("android.provider.Telephony.SMS_RECEIVED");
int i = variantHelper.getSMSPriority();
localIntentFilter1.setPriority(i);
Context localContext1 = this.myContext;
BroadcastReceiver localBroadcastReceiver1 = this.mySmsReceiver;
Intent localIntent1 = localContext1.registerReceiver(localBroadcastReceiver1, lc
SMSReceiver.2 local2 = new SMSReceiver.2(this);
this.myWAPPushReceiver = local2;
IntentFilter localIntentFilter2 = new IntentFilter();
localIntentFilter2.addAction("android.provider.Telephony.WAP_PUSH_RECEIVED");
try
{
  localIntentFilter2.addDataType("*/*");
  int j = variantHelper.getSMSPriority();
  localIntentFilter2.setPriority(j);
  Context localContext2 = this.myContext;
  BroadcastReceiver localBroadcastReceiver2 = this.myWAPPushReceiver;
  Intent localIntent2 = localContext2.registerReceiver(localBroadcastReceiver2,
```

**图 16　IQAgent.apk 接收短信和 WAP 推送信息**

checkSMS 和 checkWAPPush 实际上通过 JNI 接口调用本地代码实现。其 JNI 代码分别调用了 libiq_service_trial_x.x.so 中的 IQ_CheckSMS 和 IQ_CheckWAPPush 函数，这两个函数检查短信和 WAP 推送信息的内容，例如以“//CM”开头的短信将被屏蔽，而满足进一步条件的信息将引发该软件将搜集到的隐私信息传回服务器。

```
LDR     R2, =(gFrontend_ptr - 0xB23F8)
LDR     R3, =0xFEDC0005
ADD     R7, SP, #0x30+var_20
LDR     R4, [R4,R2]
STR     R6, [R7,#4]
STR     R3, [SP,#0x30+var_20]
ADDS    R4, #0xFC
LDR     R0, [R4,#0x38]
BL      IQPorting_CriticalSectionEnter
MOVS    R1, #8
MOVS    R0, R7
BL      IQPorting_ClientConnectionSendToServer
LDR     R0, [SP,#0x30+var_28]
MOVS    R1, R6
BL      IQPorting_ClientConnectionSendToServer
LDR     R0, [R4,#0x38]
BL      IQPorting_CriticalSectionLeave
```

**图 17　满足特定条件的短信将引起隐私回传**

在真正植入 ROM 的样本中，我们也发现了类似的代码。HtcIQAgent.apk 中申明的服务接收两个特殊的行为 com.htc.android.iqagent.action.smsnotify 和 com.htc.android.iqagent.acti

on.wapnotify，分别对应短信通知和 WAP 推送通知。这两个行为将调用 htciqagent.so 中对应的 JNI 接口，最终这些 JNI 实现还是调用了 libciq_client.so 中的 IQ_CheckSMS 和 IQ_CheckWAPPush 函数。

## 2. 动态分析

试用版软件与正式版在动态行为上有一些区别。

安装后，其软件名为 Device Health Application（图 18），有不同的图标，且所需权限也不同。


**图 18　安装到手机中的试用版软件**

该软件启动的服务名为 Device Health Service（图 19）。


**图 19　试用版软件启动的服务**

当用户或手机中的一些行为触发了该软件运行后，会在通知栏发出“DeviceHealth Monitor”的通知，点击进入后，出现一个几乎空白的界面（图 20）。

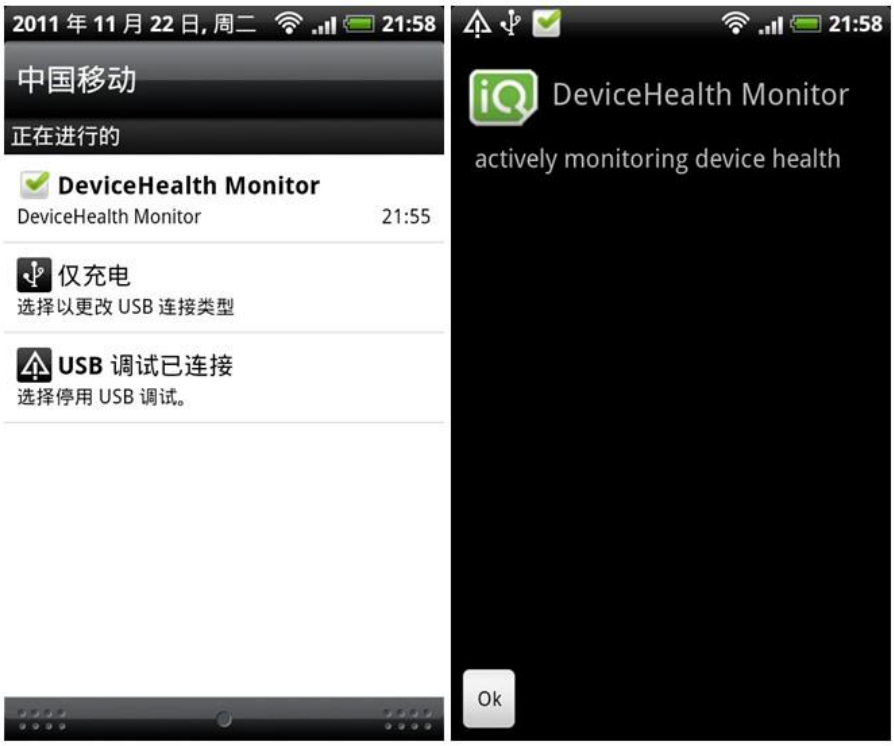



**图 20　试用版软件的提示通知和界面**

而根据相关分析 25，该软件实际上包含一个隐藏的界面（图 20），从其配置文件看，属于名为 IQ Agent Settings 的活动，且用于开发人员的调试。从界面可以看出，它包含了多种行为的记录能力。

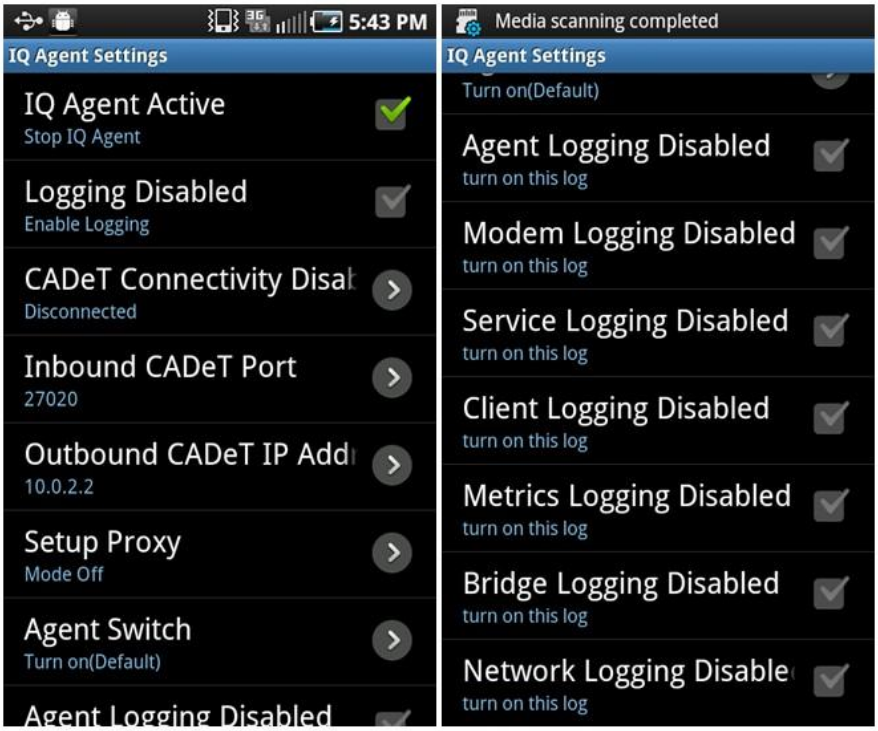


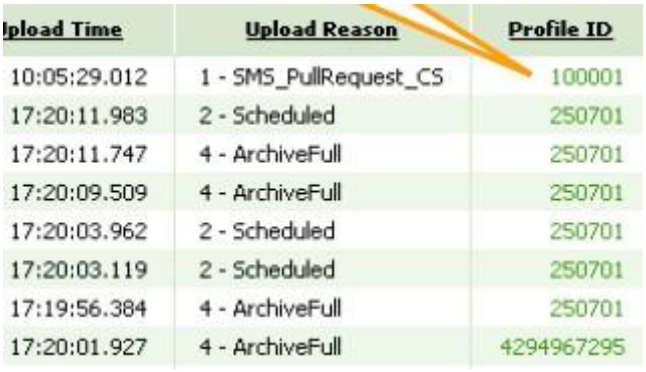

**图 21　试用版软件用于开发调试的隐藏界面**

# 六、CarrierIQ 公司资料分析

在 Carrier IQ 公司提供的后台服务产品培训资料中，可以看到以下内容：

有多种原因可以导致样本回传隐私信息（图 22），至少有：

- SMS_PullRequest_CS：特定 SMS 短信驱使，这一点与前面对代码的分析一致
- Scheduled：被调度的，猜测为定期的行为
- ArchiveFull：猜测为手机中软件为隐私信息提供的缓存已满
- PackageCreation：猜测为该软件第一次安装



| Upload Time | Upload Reason | Profile ID |
| --- | --- | --- |
| 10:05:29.012 | 1 - SMS_PullRequest_CS | 100001 |
| 17:20:11.983 | 2 - Scheduled | 250701 |
| 17:20:11.747 | 4 - ArchiveFull | 250701 |
| 17:20:09.509 | 4 - ArchiveFull | 250701 |
| 17:20:03.962 | 2 - Scheduled | 250701 |
| 17:20:03.119 | 2 - Scheduled | 250701 |
| 17:19:56.384 | 4 - ArchiveFull | 250701 |
| 17:20:01.927 | 4 - ArchiveFull | 4294967295 |

**图 22　多种原因导致样本回传隐私信息**

后台服务支持对特定 IMEI、IMSI 的查询（图 23）：

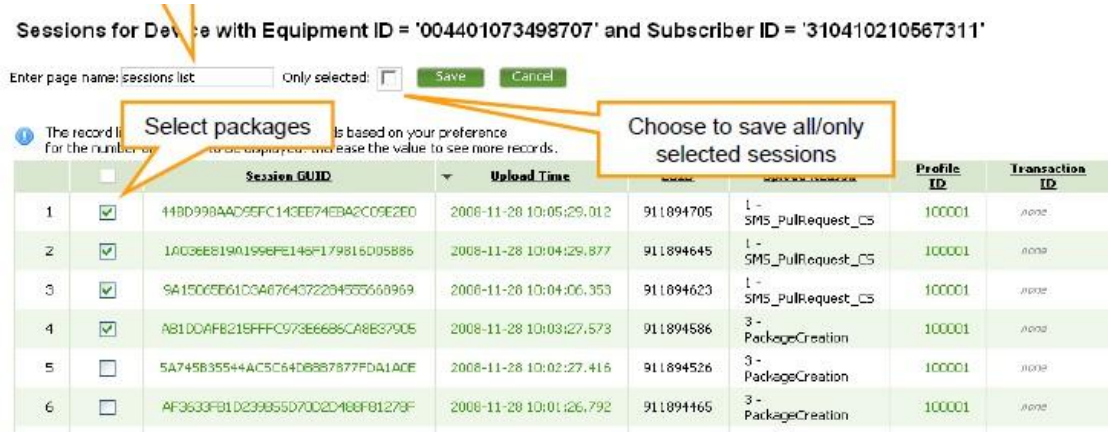



**图 23　后台产品支持 IMEI/IMSI 查询**

根据这些记录，可以看到对应手机中搜集到的 metrics，即用户行为和隐私信息记录：

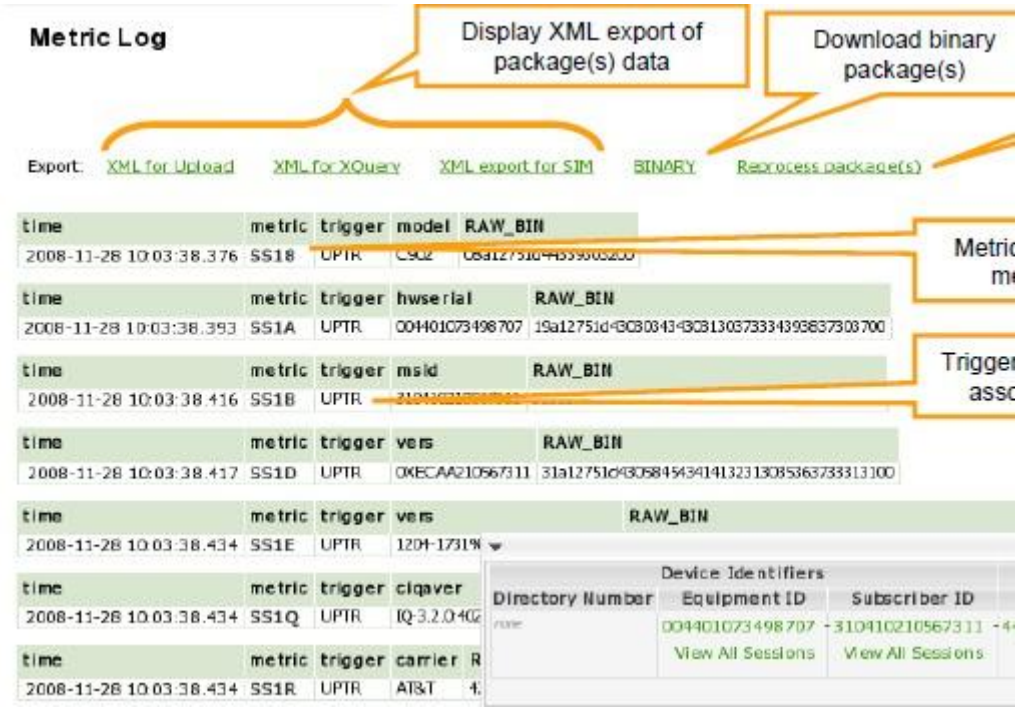



**图 24　后台产品可以查询到具体的回传记录**

对搜集到的每条记录，可以查看其具体内容：

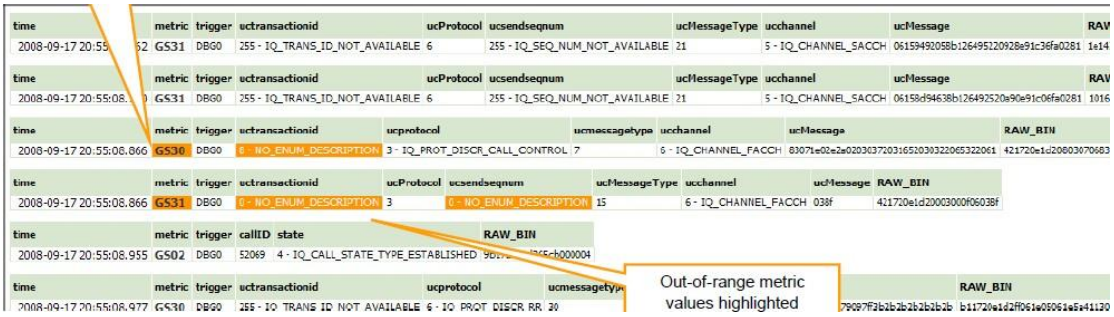
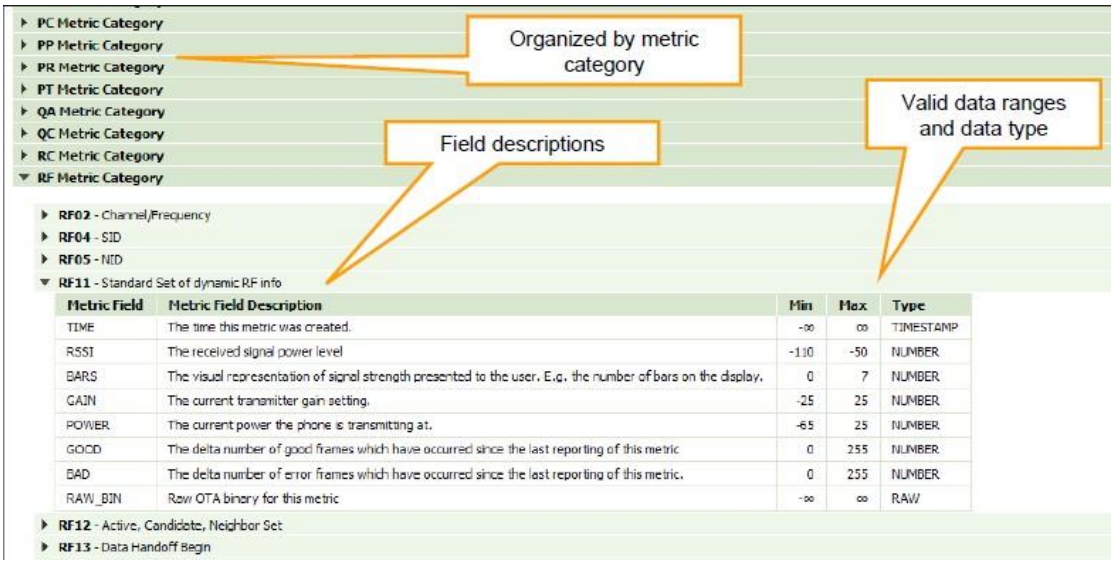



**图 25　后台产品可以查看记录具体内容**

对不同类型的记录，提供了其每个不同字段的含义解释：




| Metric Field | Metric Field Description | Min | Max | Type |
| --- | --- | --- | --- | --- |
| TIME | The time this metric was created. | -∞ | ∞ | TIMESTAMP |
| RSSI | The received signal power level | -110 | -50 | NUMBER |
| BARS | The visual representation of signal strength presented to the user. E.g. the number of bars on the display. | 0 | 7 | NUMBER |
| GAIN | The current transmitter gain setting. | -25 | 25 | NUMBER |
| POWER | The current power the phone is transmitting at. | -65 | 25 | NUMBER |
| GOOD | The delta number of good frames which have occurred since the last reporting of this metric | 0 | 255 | NUMBER |
| BAD | The delta number of error frames which have occurred since the last reporting of this metric. | 0 | 255 | NUMBER |
| RAW_BIN | Raw OTA binary for this metric | -∞ | ∞ | RAW |

**图 26　后台产品提供了记录字段的解释**

因此，通过 CarrierIQ 公司提供的后台产品，其用户可以查看到该公司客户端软件从手机中搜集到的具体隐私信息，包括针对任何特定手机的用户行为和相关隐私。

# 七、总结

从上述分析，已经可以基本确定 Carrier IQ 公司的相关手机产品存在过度的隐私搜集行为，主要体现在：

- 在不通知用户的情况下，搜集预装在 ROM 多款常用软件的使用记录和详细信息
- 在不通知用户的情况下，将这些信息回传至该公司的后台服务器
- 将这些数据本身作为产品服务提供给其企业用户

该公司的用户可以通过其后台服务，有针对性地获得具体的手机或个人的地理位置、软件使用情况等，给个人用户带来极大地潜在威胁。

该事件中另一个值得注意的是，有大型移动运营商参与到软件的传播中。一般用户认为官方预装的 ROM 是安全的，而此次样本正是被 Carrier IQ 公司与移动运营商合作预装入手机，从而具有了极大的覆盖面。运营商也许并不十分清楚这一软件的真实情况，但也应承担其应有的软件审核责任，尤其是对预装软件安全问题的审核。

# 参考文献

[1] Android Security Test. CarrierIQ. http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/

[2] Carrier IQ Corp. http://carrieriq.com/

[3] Todd Haselton. HTC Sensation and EVO 3D revealed to be spying on users. http://www.bgr.com/2011/09/01/htc-sensation-and-evo-3d-revealed-to-be-spying-on-users/

[4] Mathew J. Schwartz. Smartphone Invader Tracks Your Every Move. http://www.informationweek.com/news/security/mobile/231903096

[5] Carrier IQ Retracts Their C&D, Apologizes To The Android Researcher They Hassled. http://techcrunch.com/2011/11/23/carrier-iq-retracts-their-cd-apologizes-to-the-android-researcher/