Antiy Labs

A Comprehensive Analysis on Carrier IQ

Antiy Cert

Antiy Labs

(December 2011)

Contents

Executive Summary

Background

Recently, Android developer Trevor Eckhart found Carrier IQ software could gather user privacy information [1]. This software is pre-installed into phones by Carrier IQ and its wireless carriers.

Carrier IQ officially claims :
"Carrier IQ is the leading provider of Mobile Service intelligence Solutions to the Wireless industry. As the only embedded analytics company to support millions of devices simultaneously, we give Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience." [2]

Jason Gertzen, the spokesman of wireless carrier Sprint, claims in his mail:
It (Carrier IQ software) collects enough information to understand the customer experience with devices on our network and how to devise solutions to use and connection problems. We do not and cannot look at the contents of messages, photos, videos, etc., using this tool." [3]

However, Sprint's disclosed product patents and training material show Carrier IQ software collects network-related information, including voice and data services. It also collects other information, including device type, memory, battery, software, device location, keystroke information, and use history. Such information is uploaded to Carrier IQ's server for statistical analysis. Based on IMEI or IMSI, Carrier IQ can gather history records, so users' privacy is completely exposed to Carrier IQ and its wireless carriers.

Verizon and Sprint pre-installed Carrier IQ software in several types of phones, involving Android, Symbian and BlackBerry platforms. It is said that more than 141 million mobile phones have been infected [4]. Several well-known custom-built ROM providers, such as CyanogenMod, also use this software.

After the scandal, Carrier IQ claimed Trevor Eckhart use and backup its training materials, which infringes its rights. So, Carrier IQ sent a strongly worded cease-and-desist letter to him. However, some lawyers pointed out that Eckhart is exempted by U.S. copyright law. In November 24, Carrier IQ retracted the C&D, and re-emphasized: "(This application) does not record your keystrokes; does not provide tracking tools; does not provide real-time data reporting to any customer …Our

software is designed to help mobile network providers diagnose critical issues that lead to problems such as dropped calls and battery drain." [5]

About This Report

Antiy Labs analyzes the event and samples in depth, and draw some conclusions on Carrier IQ Trojan.

Carrier IQ Trojan is found in several custom-built ROM;
It is found in some mobile phones in China;
It is composed of several modules that are pre-installed into ROM;
It collects information on current mobile network;
It contains privacy stealing codes;
It contains codes that upload privacy to specified server;
Once executed, it would start a service;
once executed, it would trigger the uploading codes;
It uploads privacy to specified server when receiving specific-formatted SMS or WAP push messages;
It is found in trial software on 3 platforms: Android, Symbian, and BlackBerry;
CarrierIQ's product training materials indicate its software collects user privacy;
CarrireIQ can inquire information on specified phones and users, and get all detailed uploaded privacy.

Spreading Channels

Carrier IQ software has 3 trial versions on Android, Symbian S60, and BlackBerry platforms. As for Android system, it is found in the following brush ROM (Figure 1).

The official ROM that Sprint provides for HTC G3 Hero;
The official ROM that Sprint provides for HTC EVO 3D Shooter;
The Android 2.2 ROM that OMJ customizes for HTC EVO 4G;
The ROM (version 5.4 and 5.5) that Villain customizes for HTC G3 Hero;
The ROM that Synergy customizes for HTC EVO, INCredible, and MyTouch 4G.

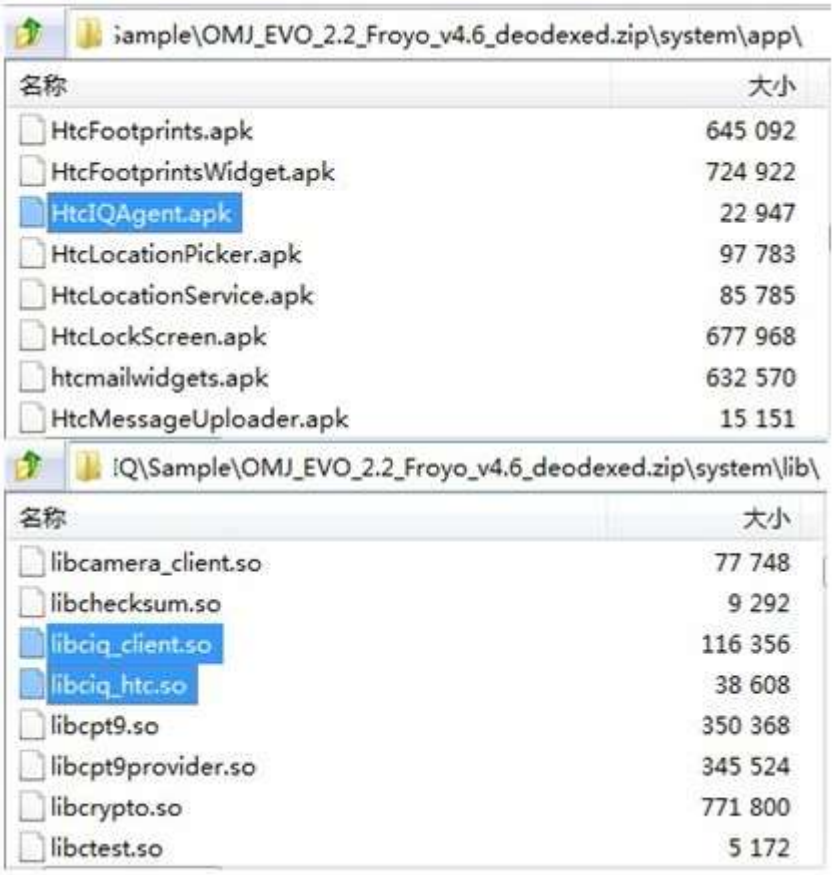

Figure1 The Software Is Found in Brush ROM

Since the second half of this year, several foreign custom-built ROM providers began removing Carrier IQ software-related components from their ROMs. Even now, we can still find residual components in some ROM. (Figure 2)

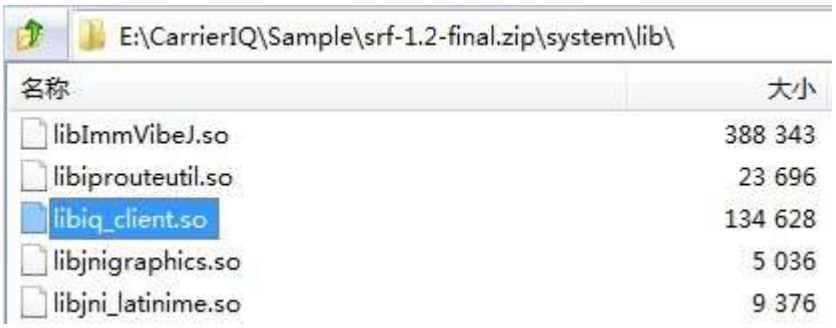

Figure2 Residual Software Components

The official ROM and custom-built ROM are mostly provided by foreign carriers or manufacturers, so they seldom contain Chinese resources. However, we find that the software is installed in some domestic phones and run for a long period. (Figure 3)

Figure3 CarrierIQ Software Is Found in Domestic Phones

Static Analysis on Samples

Software Components

In Android ROM for HTC phones, the software contains the following components:

/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

There are three APK installation files, three SO DLLs, two ELF executable files, and one configuration file “iqprofile.pro”. They are distributed under 4 directories of the ROM, and we will analyze them in detail.

APK Installation File

IQRD.apk

IQRD.apk is composed of one service com.htc.android.iqrd.IqService，one receiver com.htc.android.iqrd.StateReceiver and one activity com.htc.android.iqrd.IqActivity. It has no start menu icon. Once started, it would register two receivers (Figure 4). One receiver's trigger behavior include：

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

Another receiver's trigger behavior is as follows:

com.android.phone.MESSAGE_SENT

We are not sure which programs trigger the behavior above.

```
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,
```

Figure 4 Receivers Registered by IQRD.apk

IQRD.apk needs additional privileges as follows:

CALL_PHONE：allow applications to dial without user intervention;

READ_PHONE_STATE：allow applications to access phone functions, determining phone number, serial number, whether on a call, and the other side's number；

SEND_SMS：allow applications to send messages；

CHANGE_NETWORK_STATE: allow applications to change network connection state.

IQRD.apk uses a special property: android:sharedUserId="android.uid.phone". It has the same signature with Phone.apk, the application that is responsible for phone call. Then, IQRD.apk and Phone.apk will run with the same UID, so two sides can mutually get the other's data.

The CDMA version can read network ESN, MEID, MDN, MSID, PRL, SPN, MIP, NAI, etc., including NAI user name and passwords (Figure 5). Its GSM version can read network-related information, such as MCC, MNC, APN, etc.

```
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);
}
```

Figure 5 IQRD.apk Reads NAI Passwords

HtcIQAgent.apk

It has only one service com.htc.android.iqagent.AgentService, which can be triggered by 25 acts that are similar to com.htc.android.iqagent.action.ss1c, which is is actually associated with the pre-installed software.

Further analysis on the code indicates that Carrier IQ names triggered objects as metric, which matches the naming in official training materials and patents. Specifically speaking, it sets an integer for some pre-installed software as an identifier. (Figure 6) Then, it uses byteToHexString and hexStringToByteth to match these integers with a metric, and associate trigger acts such as com.htc.android.iqagent.action.ss1c with different software.

```
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;
```

Figure 6 HtcIQAgent.apk Sets Mapping for Software

Associated pre-installed software includes:

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

Based on different trigger acts, it gets corresponding applications, and then collects privacy information, such as specific GPS positions, etc. (Figure 7)

Once HtcIQAgent.apk gets such information, it will call local htciqagent.so file and provide corresponding JNI interfaces to upload privacy to specified server.

```
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";
```

Figure 7 HtcIQAgent.apk Collects GPS Information

SO DLL

HtcIQAgent.apk calls JNI interface provided by htciqagent.so, which is actually an encryption layer and contains two types of functions (Figure 8). One type is JNI interface provided for APK and is like Java_com_htc_android_iqagent_Controller_submitAL16. It can call internal functions like actionAL16. These action functions get privacy data respectively and piece them together, then, they call IQ_SubmitMetric to upload the data and send information sources as a parameter to JNI interface.

Figure 8 Some Functions of Htciqagent.so

IQ_SubmitMetric is realized in libciq_client.so. It first calls iq_metric_might_be_interesting to judge whether the data are interesting. If they are, it will get the current timestamp, and then calls iq_submit_metric to upload data.

Configuration Files

File iqprofile.pro is pre-installed under /system/etc of the ROM, and then is encrypted. But, it contains a partially plain-text URL as follows:

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

Its subdomain is “collector”.

iqprofile.pro is called by executable file iqd.

ELF Executable File

Executable file iqd contains the following URL：
http://collector.sky.carrieriq.com:7001/collector/c?cm_sl=5

Dynamic Analysis on Samples

In phones with Carrier IQ software, “all applications” list contains programs named HTC IQAgent and IQRD (Figure 9). Privileges that IQRD needs are shown in Figure 10.

It should be noted that IQRD needs more privileges in ROM than in AndroidManifest.xml. The additional privileges are as follows:

Read and modify contact information;
Edit, read, and receive SMS and MMS;
Get rough positions based on network;
Create Bluetooth connection and internet access;
Change voice settings;
Manage Bluetooth; change Wi-Fi states and UI settings; modify system global setting; set time, and modify APN setting.
IQRD uses a shared UID android.uid.phone, so it can use privileges in system program com.android.phone.

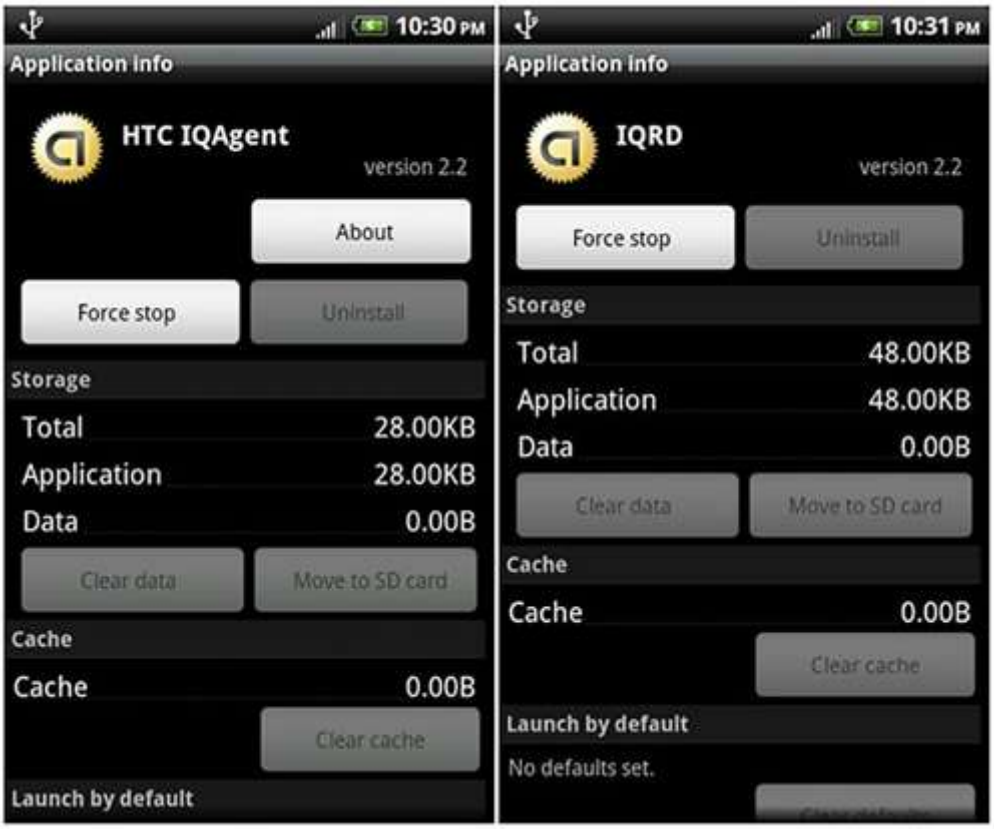

Figure 9 Corresponding Applications

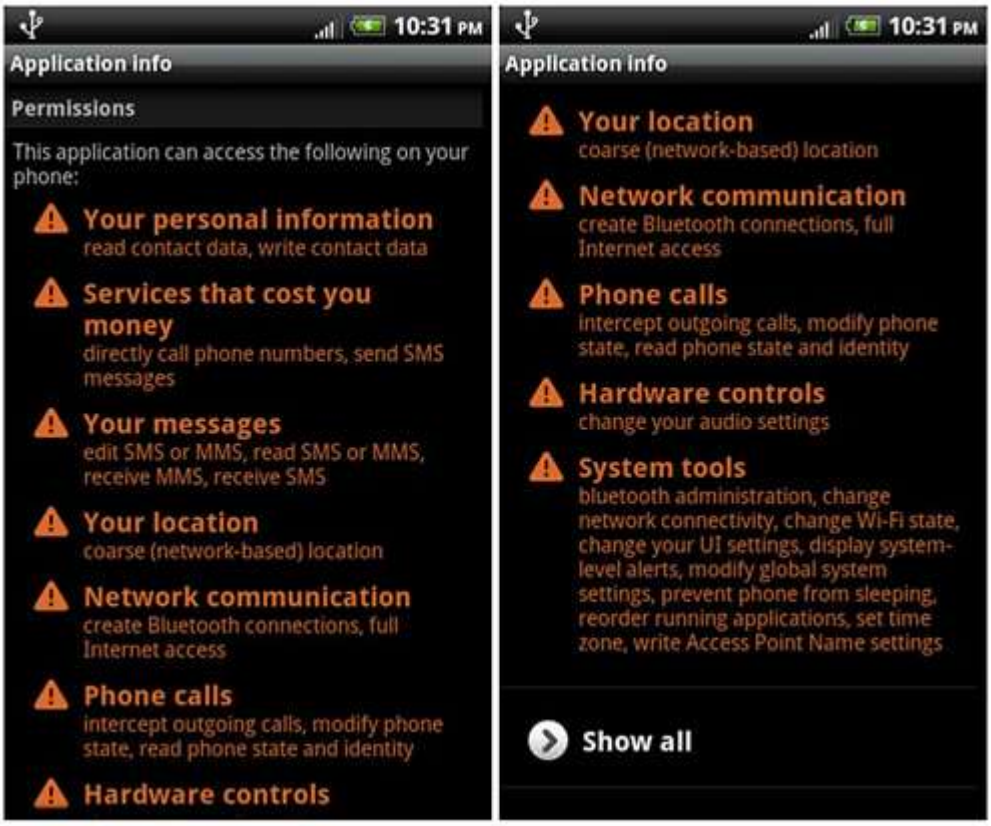

Figure 10 Privileges IQRD Needs

The sample software would start program AgentService. (Figure 11)

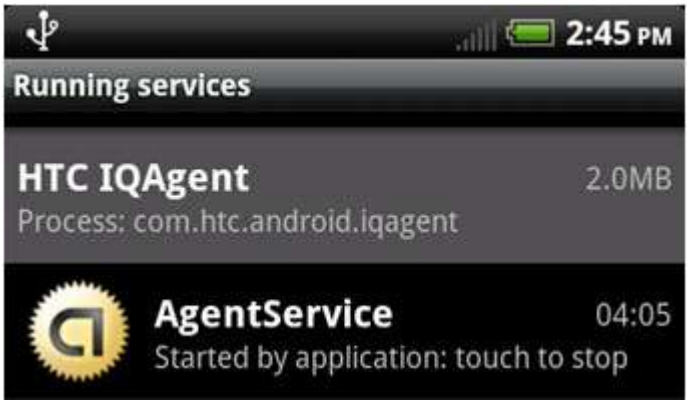

Figure 11 Services Started by HtcIQAgent

When users access a webpage, or start a Google search, the sample will output debugging information (Figure 12), which is output by residual debugging code in htciqagent.so file and located in JNI interface Java_com_htc_android_iqagent_Controller_submitAL15 (Figure 13). The JNI interface is called after HtcIQAgent.apk collects Web access related privacy data.

However, no privacy uploading related network data are captured.

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

```
 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]
```

Figure 13 Residual Debugging Information in Htciqagent.so

Analysis on Trial Version Software

Carrier IQ software has trial versions on three platforms: Android, Symbian, and BlackBerry.

IQAgent.apk: used in Android system;
IQ_AgentVM_S603rdMRd.sisx: used in Symbian S60 system;
IQAgent.cod: used in BlackBerry 4.7.0 system.
It should be stressed that analysis on this sample has been available on network [1], but mainly on the trial version. Though the trial version and the official version have many similarities, they are quite different in user behavior, which will be described in detail later.

The following is analysis on Android version.

Static Analysis

It needs many running privileges, including:

INTERNET: allow applications to create a network socket;
READ_PHONE_STATE：allow applications to access phone functions, determining phone number, serial number, whether on a call, and the other side's number；
RECEIVE_BOOT_COMPLETED：allow applications to auto-start after the system boots;
RECEIVE_SMS: allow applications to receive and process messages;
MODIFY_PHONE_STATE: allow applications to control phone functions without notifying users, including network switching, wireless communications on/off.
CHANGE_NETWORK_STATE: allow applications to change network connection states;
GET_TASKS：allow applications to retrieve current/ recent tasks. Malicious applications can thereby get privacy information;
ACCESS_NETWORK_STATE：allow applications to check all networks' states;
ACCESS_COARSE_LOCATION：access rough positions to locate phones;
ACCESS_FINE_LOCATION：access precise positions, such as GPS;
ACCESS_WIFI_STATE：allow applications to check Wi-Fi states;
READ_LOGS：allow applications to read information from various system log files, thereby, applications can find privacy information;
RECEIVE_WAP_PUSH：allow applications to receive and process WAP information;
PERSISTENT_ACTIVITY：allow applications to partially run, so they can't be applied to other applications;
PROCESS_OUTGOING_CALLS：allow applications to process outbound calls or change numbers to be dialed; malicious applications can thereby monitor, transfer, or even prevent outbound calls;
WAKE_LOCK：allow applications to prevent phones sleeping;
BATTERY_STATS：allow applications to modify collected battery statistics; ordinary applications don't have this privilege.
When the phone screen is on/off, the system boots, or the battery states change, the receiver com.carrieriq.trial.service.receivers.BootCompletedReceiver is triggered and starts com.carrieriq.trial.service.IQService.

Based on system versions, IQService calls one of the two dropped local library files: libiq_service_trial_1.6.so and libiq_service_trial_2.2.so.

```
CIQHTTPUploadTransactionProvider::CIQHTTPUploadTransactionPr...
CIQHTTPUploadTransactionProvider::CIQHTTPUploadTransactionPr...
CIQHTTPUploadTransactionProvider::Initialize(void (*)(void *),void (...
CIQHTTPUploadTransactionProvider::NetworkSubscriber::IssueArri...
CIQHTTPUploadTransactionProvider::NetworkSubscriber::~Networ...
CIQHTTPUploadTransactionProvider::NetworkSubscriber::~Networ...
CIQHTTPUploadTransactionProvider::NotifyNetworkFailure(void)
CIQHTTPUploadTransactionProvider::NotifyNetworkReadyCallback(...
CIQHTTPUploadTransactionProvider::OpenTransaction(char const*,...
CIQHTTPUploadTransactionProvider::Shutdown(void)
```

Figure 14 Libiq_service_trial_2.2.so Realizes HTTP Uploading

The sample detects outbound calls and forbids the call when the number is "#*47234#", which is USSD code of wireless carriers.

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

Figure 15 IQAgent.apk Forbids Calling Specific Number

In addition, this sample creates two receivers to receive android.provider.Telephony.SMS_RECEIVED and android.provider.Telephony.WAP_PUSH_RECEIVED broadcast. When it receives SMS or WAP push messages, it will call checksums and checkWAPPush to check them. Specific messages won't be displayed.

```
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,
```

Figure 16 IQAgent.apk Receives SMS and WAP Push Messages

Actually, JNI interface calls local codes to realize checksums and checkWAPPush. The JNI code calls functions IQ_CheckSMS and IQ_CheckWAPPush from libiq_service_trial_x.x.so. The two functions check SMS and WAP push messages. For example, SMS started by "//CM" will be blocked, and condition-satisfied information will be uploaded to specified server.

```
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
```

Figure 17 Specific SMS Are Uploaded

In official ROM samples, we find similar codes. Stated services in HtcIQAgent.apk receive two special acts com.htc.android.iqagent.action.smsnotify and com.htc.android.iqagent.action.wapnotify, which respectively correspond to SMS notification and WAP push notification. The two acts call corresponding JNI interface of

htciqagent.so. Finally, JNI interface calls functions IQ_CheckSMS and IQ_CheckWAPPush from libciq_client.so.

Dynamic Analysis

The trial version and official version are somewhat different in dynamic acts.

After installed, they are named Device Health Application (Figure 18). They have different icons and privileges.

Figure 18 Trial Version Installed in Phones

It starts a service named Device Health Service (Figure 19).

Figure 19 The Service Started by Trial Software

Triggered by some user or phone acts, the software will give a “DeviceHealth Monitor” notification. Click enter, an almost blank interface is seen.

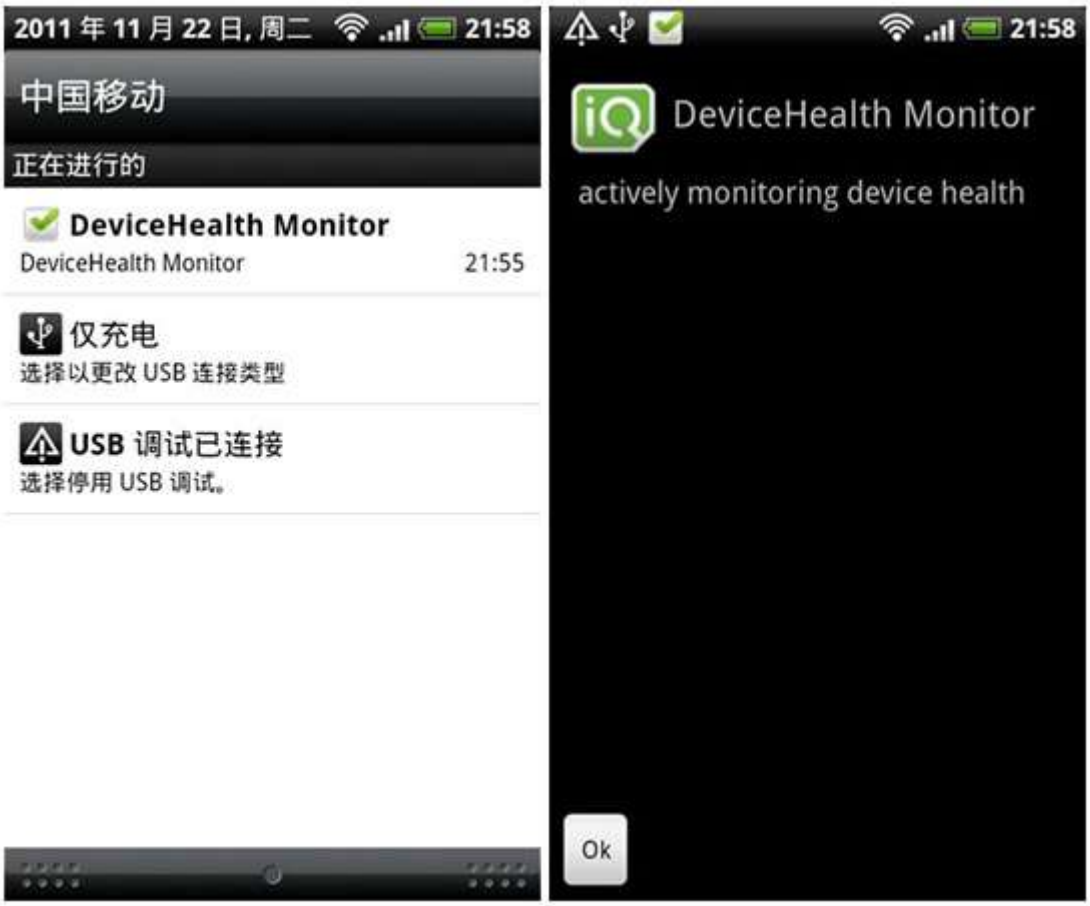

Figure 20 Notification and Interface (Trial Software)

According to related analysis, this software actually contains a hidden interface (Figure 20). From its configuration files, we know the interface is IQ Agent Settings and is used to debug. Moreover, it can record many acts.

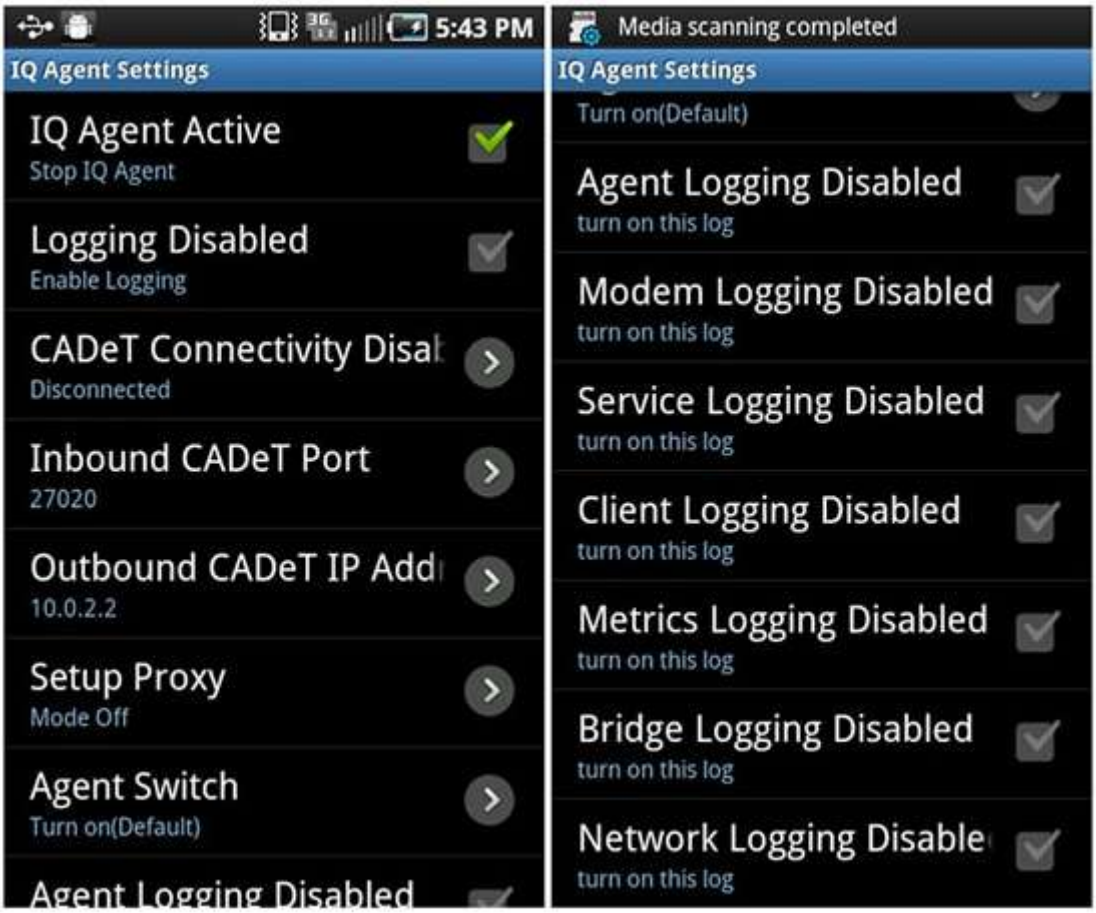

Figure 21 Hidden Interface Used for Debugging (Trial Software)

Analysis on CarrierIQ Materials

From the training materials of Carrier IQ, we find that several reasons cause privacy uploading (Figure 22).

SMS_PullRequest_CS: triggered by specific SMS, which is mentioned earlier;
Scheduled：scheduled and speculated to be periodic acts;
ArchiveFull：the cache for privacy information is speculated to be full;
PackageCreation：the software is speculated to be first installed.

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

Figure 22 Several Reasons Cause Privacy Uploading

Support products inquire specific IMEI and IMSI. (Figure 23)

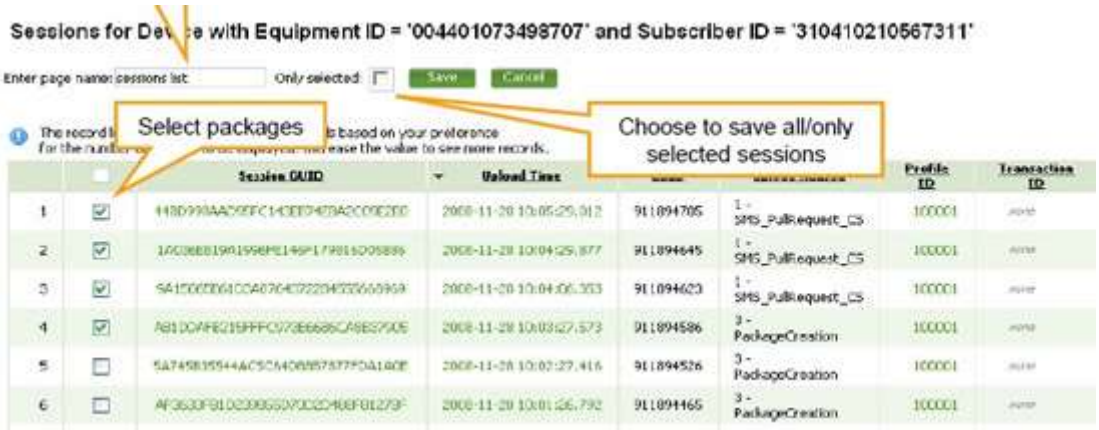

Figure 23 Support Products Inquire IMEI/IMSI

Based on these records, corresponding metrics can be found, i.e. user behavior and privacy records.

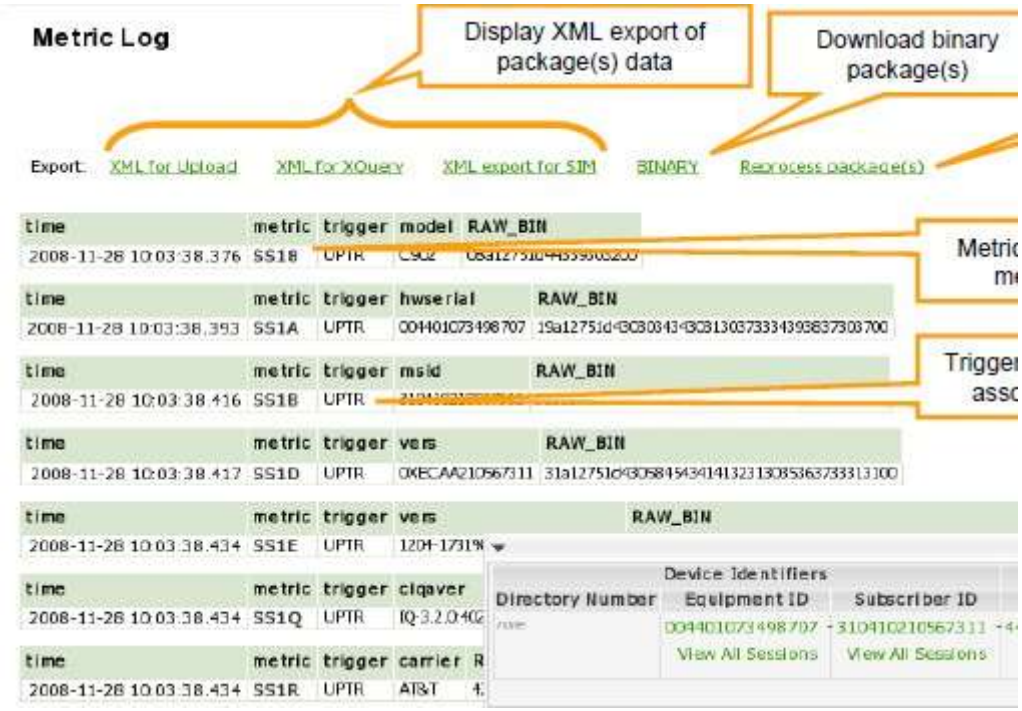

Figure 24 Support Products Inquire Specific Uploaded Records

Detailed information of every record can be read.

Figure 25 Support Products Inquire Detailed Information

For different types of records, description of every filed is provided.

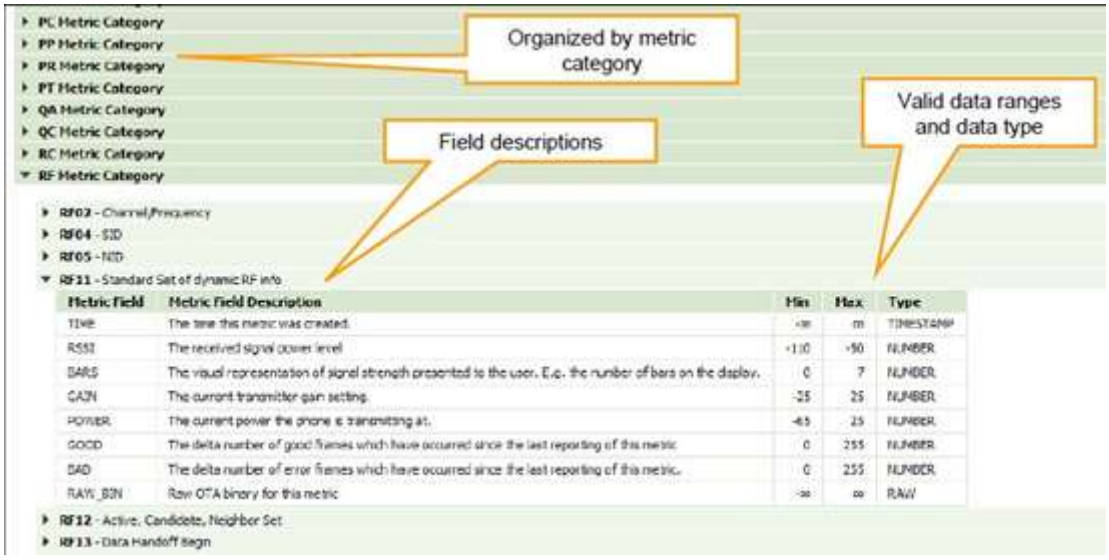

Figure 26 Support Products Provide Filed Description

Therefore, through support products that Carrier IQ provides, users can get specific privacy information collected by the software, including user acts and related privacy of any specified phone.

Event Follow-Up Progress

On November 29, we released the first edition of this report. Thereafter, many institutes both home and abroad responded to the event.

On November 29, Trevor Eckhart published a video, showing how Carrier IQ software run in phones and get privacy information [6] .

On November 30, researchers found Carrier IQ software in Apple's iPhone, including iOS 3.1.3, iOS 4 and the latest iOS 5. [7]

On December 1, Lookout claimed in a blog that it had received user request of knowing real situations of Carrier IQ. It believed Carrier IQ software was not malware. [8]

The same day, RIM claimed they never pre-installed Carrier IQ software into BlackBerry, nor allowed partner carrier to do so. The Carrier IQ software users found in BlackBerry was installed by themselves; or else, it was installed and authorized by the administrator of BlackBerry Enterprise Server. [9]

Nokia claimed no Carrier IQ would be installed in any phone. [10]

Later, Apple claimed they once used Carrier IQ network diagnostic software, but they would delete it in time. “We never recorded keystrokes, messages or any other personal information for diagnostic data and have no plans to ever do so.”[11]

Also on December 1, AT&T, Sprint, T-Mobile, and other carriers confirmed that they installed Carrier IQ software in their phones. AT&T and Sprint said they wanted to improve wireless network. T-Mobile said they never used the software to collect user SMS, email. etc. Verizon denied using Carrier IQ software, and claimed they never customized pre-installed Carrier IQ software. [12]

The same day，HTC and Samsung confirmed they installed Carrier IQ in their phones, but claimed they did so to satisfy carriers. [12]

Finally, Carrier IQ claimed the software ignored personal information. [13]

On December 2, the data protection institute in Bavaria, Germany launched questions on Carrier IQ issues to Apple. [14]

The same day, American representative Edward Markey asked Federal Trade Commission (FTC)to investigate whether Carrier IQ invaded user privacy [15] .

On December 3, Carrier IQ, HTC and Samsung were accused in Missouri, Illinois and some other regions. [16] Up to now, no carrier has been accused.

Summary

Based on the analysis above, we are sure that the phone software Carrier IQ provides collects user privacy information:

Without notifying users, it collects use records and detailed information of the software pre-installed in ROM.
Without notifying users, it uploads privacy to Carrier IQ server.
Carrier IQ provides user privacy information for enterprise customers.
Through Carrier IQ’s support service, enterprise users can get positions of specified phones and its installed software, therefore, Carrier IQ software greatly threatens individual user security.

One more thing should be noted: large mobile carriers are involved in Carrier IQ software spreading. Ordinary users believe official pre-installed ROM is secure, but the software is just pre-installed into phones by Carrier IQ and its mobile carriers, so it has a

great coverage. Carriers may not be well aware of the software, but they should be responsible for its audit, especially security audit for pre-installed software.

References

(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/**

(6). Russell Holly. Security researcher responds to CarrierIQ with video proof. **http://www.geek.com/articles/mobile/security-researcher-responds-to-carrieriq-with-video-proof-20111129/**

(7). Dieter Bohn. Carrier IQ references discovered in Apple's iOS. **http://www.theverge.com/2011/11/30/2601875/carrier-iq-references-discovered-apple-ios-iphone**

(8). Lookout. Our Take on Carrier IQ. **http://blog.mylookout.com/2011/12/our-take-on-carrier-iq/**

(9). MSohm. Re: Does CarrierIQ run on BlackBerry devices?. **http://supportforums.blackberry.com/t5/Java-Development/Does-CarrierIQ-run-on-BlackBerry-devices/m-p/1439275#M183840**

(10). Vlad Savov. Nokia: none of our devices have ever used Carrier IQ. **http://www.theverge.com/2011/12/1/2602502/nokia-none-of-our-devices-have-ever-used-carrier-iq/in/2365736**

(11). John Paczkowski. Apple: We Stopped Supporting Carrier IQ With iOS 5. **http://allthingsd.com/20111201/apple-we-stopped-supporting-carrieriq-with-ios-5/**

(12). Jaikumar Vijayan. AT&T, Sprint confirm use of Carrier IQ software on handsets. **http://www.computerworld.com/s/article/print/9222319/AT_T_Sprint_confirm_use_of_Carrier_IQ_software_on_handsets**

(13). John Paczkowski. Carrier IQ Speaks: Our Software Ignores Your Personal Info. **http://allthingsd.com/20111201/carrier-iq-speaks-our-software-monitors-service-messages-ignores-other-data/?reflink=ATD_yahoo_ticker**

(14). Bavaria asks Apple to answer questions on Carrier IQ. **http://www.electronista.com/articles/11/12/02/state.may.accept.apple.promise.to.drop.software/**

(15). Congressman asks FTC to investigate Carrier IQ.**http://www.electronista.com/articles/11/12/02/ftc.asked.to.see.what.carrier.iq.knows/**

(16). HTC 三星 Carrier IQ 违反窃听法遭集体诉讼. http://it.sohu.com/20111203/n327792995.shtml

(17). Lookout. Carrier IQ Detector Released. **http://blog.mylookout.com/2011/12/carrier-iq-detector-released/**

(18). Ryan Singel. Dropbox Lied to Users About Data Security, Complaint to FTC Alleges. **http://www.wired.com/threatlevel/2011/05/dropbox-ftc/**

Revision History

Version 1.0 (Nov 29, 2011)

•Version 1.0 was released.

Version 1.0 (Dec 2, 2011)

•Version 1.0 was published.

Version 1.1 (Dec 4, 2011)

- Version 1.1 was published.
- Added the “Event Follow-Up Progress” section

Version 1.1 (Dec 5, 2011)

- Version 1.1(English version) was published.

About Antiy Labs

Antiy Labs is an antivirus vendor which makes advanced research and technology contributions to the field. Currently, there are tens of thousands of firewalls, UTM and security devices deployed with our antivirus engine. More information is available at www.antiy.net.

ANTIY | Antiy Labs