

Antiy Cert

Antiy Labs

(December 2011)

# Contents

Executive Summary	1
Background	
About This Report	2
Spreading Channels	2
Static Analysis on Samples	4
Software Components	4
APK Installation File	5
IQRD.apk	5
HtclQAgent.apk	6
SO DLL	9
Configuration Files	9
ELF Executable File	
Dynamic Analysis on Samples	10
Analysis on Trial Version Software	13
Static Analysis	
Dynamic Analysis	17
Analysis on CarrierIQ Materials	19
Event Follow-Up Progress	22
Summary	23
References	24
Revision History	25
Version 1.0 (Nov 29, 2011)	25
Version 1.0 (Dec 2, 2011)	25
Version 1.1 (Dec 4, 2011)	



# **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. ANTIY Antiy Labs

A Comprehensive Analysis on Carrier IQ

名称	大小
HtcFootprints.apk	645 092
HtcFootprintsWidget.apk	724 922
HtcIQAgent.apk	22 947
HtcLocationPicker.apk	97 783
HtcLocationService.apk	85 785
HtcLockScreen.apk	677 968
htcmailwidgets.apk	632 570
HtcMessageUploader.apk	15 151
IQ\Sample\OMJ_EVO_2.2_Froyo_v4.6	_deodexed.zip\system\li
名称	大小
libcamera_client.so	77 748
libchecksum.so	9 292
libciq_client.so	116 356
libciq_htc.so	38 608
libcpt9.so	350 368
	345 524
libcpt9provider.so	
	771 800

#### 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)

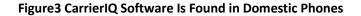
🦻 📙 E:\CarrierIQ\Sample\srf-1.2-fin	2-final.zip\system\lib\			
名称	大小			
libImmVibeJ.so	388 343			
📄 libiprouteutil.so	23 696			
libiq_client.so	134 62			
libjnigraphics.so	5 036			
libjni_latinime.so	9 376			

#### 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)

A Comprehensive Analysis on Carrier IQ

2.1系统型HtcIQagent是什么软件,有什么」 ③ NtcIQagent。软件、系段 如题,看着很不更,太质型,想加数,他出词强		发表于 2010-4-25 10:58 说料 个人空峰 整满是 加力好友 自沙~ 补充一个: 1、进程管理开启时, 里面有个HttclQagent,这个是干什么用的?
发表于 2010-5-16 11:58 资料 个人空阔 壁涧燈 加	为好友	
整寻无果 请教如何删除Htc3QAgent HtclQAgent 数是那个开锁屏后划图才可以进 thanks oza	II         IS           01.         05-05         16:40:17.20           (1485):         No         20mge           02.         05-05         16:40:17.30           03.         05-05         16:40:17.30           04.         05-05         16:40:17.30           05.         06-05         16:40:17.30           05.         06-05         16:40:17.30           05.         08-05         16:40:17.30	proid.igagent.AgentService940671760 onStartCommand:Intent { act-com
[求助] 清何解了Evo 2.3后总是出现H		。 m.htc.android.iqagent)已意外停止?



# **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/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

 $com. and roid. phone. {\tt HtcCdmaPhoneApp.NAI\_INFO}$ 

Another receiver's trigger behavior is as follows:

com.android.phone.MESSAGE\_SENT

We are not sure which programs trigger the behavior above.

```
IntentFilter localIntentFilter! = new IntentFilter("com.android.phone.HtcCdmaPhoneApp.WAKE_CIQ");
localIntentFilter!.addAction("com.android.internal.policy.impl.SHUTDOWN_CIQ");
localIntentFilter!.addAction("com.android.phone.HtcCdmaPhoneApp.DISABLE_CIQ");
localIntentFilter!.addAction("com.android.phone.HtcCdmaPhoneApp.NAI_INFO");
Context localContext2 = this.mContext;
BroadcastReceiver localBroadcastReceiver! = this.mFDReceiver;
Randler localBrandler! = this.mEndler;
Intent localIntent! = localContext2.registerReceiver(localBroadcastReceiver!, localIntentFilter],
```

#### 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 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

#### HtclQAgent.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.

A Comprehensive Analysis on Carrier IQ

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

#### Figure 6 HtclQAgent.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 HtclQAgent.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 19 = 65535L;
long 110 = localIntent15.getLongExtra(str32, 19);
Intent localIntent16 = localIntent1;
String str33 = "Longitude";
```

Figure 7 HtclQAgent.apk Collects GPS Information



#### SO DLL

HtclQAgent.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.

Java\_com\_htc\_android\_iqagent\_Controller\_submitNT1C Java\_com\_htc\_android\_igagent\_Controller\_submitNT07 Java\_com\_htc\_android\_igagent\_Controller\_submitUI08 f Java\_com\_htc\_android\_iqagent\_Controller\_submitSS1C f Java\_com\_htc\_android\_iqagent\_Controller\_submitSS1U f Java\_com\_htc\_android\_iqagent\_Controller\_submitSS1V Java\_com\_htc\_android\_iqagent\_Controller\_IQInit actionWAPPush actionSMS actionUI12 actionUI09 f actionHW03 f actionLC18 actionNT1C actionNT07

#### 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.

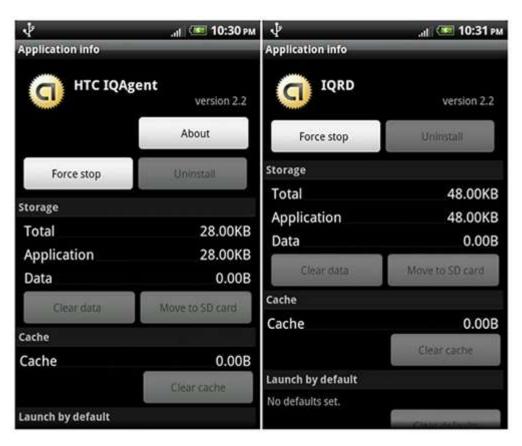
It should be noted that IQRD needs more privileges in ROM than in AndroidManifest.xml. The additional privileges are as follows:

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. IORD uses a shared UID android uid phone, so it can use privileges in system program.

IQRD uses a shared UID android.uid.phone, so it can use privileges in system program com.android.phone.

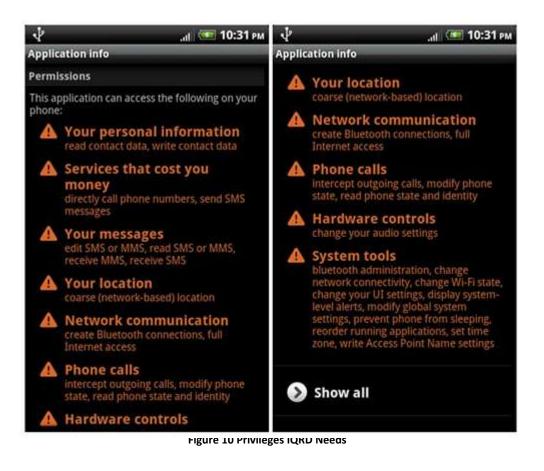
ANTIY Antiy Labs

A Comprehensive Analysis on Carrier IQ



**Figure 9 Corresponding Applications** 

A Comprehensive Analysis on Carrier IQ



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

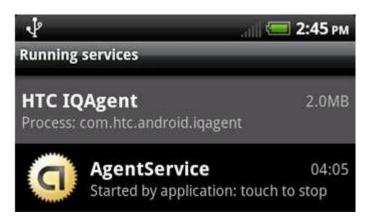


Figure 11 Services Started by HtclQAgent

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 HtclQAgent.apk collects Web access related privacy data.

ANTIY Antiy Labs

A Comprehensive Analysis on Carrier IQ

However, no privacy uploading related network data are captured.

Application	Tag	Text
com.htc.android.iqagent	dalvikvm	NO JNI_UnLos
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

#### 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_1700
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"
MOUS	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.



#### 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.

A Comprehensive Analysis on Carrier IQ

```
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.

<b>14 14 1</b> 2	3
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
MOUS	R1, #8
MOUS	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 HtclQAgent.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).

A Comprehensive Analysis on Carrier IQ



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.



🚓 🗿 🛛 🖓 🖏 🗤 🗰 🖓	:43 PM	👼 Media scanning completed	
IQ Agent Settings		IQ Agent Settings	
IQ Agent Active Stop IQ Agent	$\checkmark$	Turn on(Default)	
Logging Disabled		Agent Logging Disabled	$\checkmark$
Enable Logging	1020	Modem Logging Disabled	$\checkmark$
CADeT Connectivity Disal: Disconnected	>	Service Logging Disabled	M
Inbound CADeT Port	>	turn on this log	020
Outbound CADeT IP Add	>	Client Logging Disabled	$\checkmark$
10.0.2.2	2	Metrics Logging Disabled	
Setup Proxy Mode Off	>	Bridge Logging Disabled	-
Agent Switch	>	turn on this log	$\checkmark$
Turn on(Default)		Network Logging Disable	$\square$
Agent Logging Disabled	-1		

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. ANTIY Antiy Labs

A Comprehensive Analysis on Carrier IQ

Ipload 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)

	2	ossions list Only si		Save	Garcel				
	record is	Select packages	is based on your	r préfer te serrir	once sore records,		o save all/only d sessions	in the second	
		Seasien GUI	2	*	Valored Times			Profile ID	Transaction
1	Ð	4480998AA592FC143EE94	TRADCORDEDED	2058	11-20 10:05:29,012	911894705	1+ SMS_Pulkequest_CS	100001	.0010
2	$\square$	100308819019969814991	79815005885	2008	-11-20 10(04:25,877	911894645	L+ SH5_PullEequest_C5	100001	-
3	<u>()</u>	SA1506006100487640722	1940325669959	2008	-11-00-10:04:00:353	911094620	1 - SMS_PuBlequest_CS	100001	100
4	R	AB1DOAFE219FFC073E6	RECAGES750E	2008	11-28 10:03:27.573	911894586	3 - PackageCreation	100001	1010
5		5A745835544AC5C540835	7377FDA140E	2007	-11-28 10:02:27.416	911894526	3 - PadkageCreation	100001	1000
6		AF3630F91023995507303	10406F81279F	2008	-11-20 10:01:26.792	911894465	3 - PackageCreation	100001	1000

#### Figure 23 Support Products Inquire IMEI/IMSI

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

A Comprehensive Analysis on Carrier IQ

Metric Log		-	Di	)ownload binary package(s)		
Export XML for Upload	XML	for XQue	Y XML	expert for SIM BII	NARY REPORTS	package(s)
time	metric	trigger	model R/	W_BIN		
2008-11-28 10:03:38.376	SS18	UPIR	C902 08	412751044559505250		Metri
time	metric	trigger	hwserial	RAW_BIN		m
2008-11-28 10:03:38,393	SS1A	UPTR	0044010734	98707 19a12751d430803	343430313037333439383	7303700
time	metric	trigger	msid	RAW_BIN		Trigge
2008-11-28 10:03 38 416	SS18	UPIR 🗕	2104303170	CANTER STREET		asso
time	metric	trigger	VEIS	RAW_BIN		
2008-11-28 10:03:38 417	SS1D	UPTR	OKECAA210	567311 31a12751043058	845434141323130853637	33313100
time	metric	trigger	Vers	RA	W_BIN	
2008-11-28 10:03 38.434	SS1E	UPTR	1204-1731%	*		
time	metric	trigger	cigaver		Device Identifiers	
2008-11-28 10 03:38.434		UPTR	IQ-3.2.0.402	Directory Number		Subscriber ID - 310410210567311 - 4
time	metric	trigger	carrier R		View All Sessions	View All Sessions
2008-11-26 10:03 38:434		UPTE	AT&T 4			

Figure 24 Support Products Inquire Specific Uploaded Records

Detailed information of every record can be read.

time	matric	<b>Sripper</b>	actramactionid	ucProtocol	scandoopen		acHeesapeType.	acchannel	scHessage	R/
2008-09-17 20:55 52	G\$31	0000	288 - 10_TRANS_ID_NOT_AVAI	LABLE 6	255-10_580_NUM	NOT_AVAILABLE	21	1-10, DHANNEL, SACO	012104900985-026495209	1426493c74640381 34
tme	metric	tripper	sctramactionid	ucProtocol	acumduoquan		actionsage7ype	acthannel	ur.Honsays	
2008-09-17 20 59-08	6633	2868	38- 10_TRAVE_ID_NOT_AVAI	DABLE 8	HIS - TO_SEQ_NUM	NOT_AVAILABLE	28	S-SQ_DAMAB_SACO	0.515-04636-0548202	second second
time	matrix	irigger	advantantional .	epoteci			theread	orthorage		RAW_BEN
2008-09-17 20 53:00.096	6130	2000	sea made decomposed	3-32_AROT_DODCA	CALL_CONTROL 7	5	10, CHANNEL, FA	00+ 83075+00+3+000007	003-0530000230003220013	421720+1-008038704
time .	matrix	trigger.	extramentionid .	aProtocal married	-	out the superTry	lemetre e	unHennage R	AW_BEH	
2008-09-17 20 55:08.865	6531	0850	CONTRACT STREET OF	1 100	In the second second	15	6-12_04MAE	LFACCH 0387 4	11720+1-120012000104038+	
time //	metric	tripper	caliDD state		RAW_BIN					
2008-09-17 20 55:08.955	6501	5860	12068 4-10_CALL_STATE_TY	PE_ESTABLISHED	Run 14/100000		-			
time	metric	tripper	ectramactionid	ugretocol	- working	and the second se	ut-of-range	1047490D	RAW_B	ы
2008-09-17 30 55-06 977	-		285 - DO TRAVE 10 NOT AVAI	LABLE 4-10 PROT	CONTRACTOR AND DO		values highlight	there here	the rest of the local states of	statute teners - P. of

Figure 25 Support Products Inquire Detailed Information

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

ANTIY Antiy Labs

A Comprehensive Analysis on Carrier IQ

PP Hetric Categor PR Metric Categor		nic		
PT Hetric Categor				Valid data ranges
QA Hetric Categor				
QC Metric Category Field descriptions				and data type
RC Metric Categor	۷ <u>لیست</u>			
<b>RF Metric Categor</b>	Y			
+ Rf02 - Charnel	hwaverey			1/
> REF04 - SID				V
> RE05-ND				V
* RF11-Standard	Set of dynamic RF info			
Hetric field	Hetric field Description	Hin	Hex	Туре
TINE	The time this reactic was created.			TIMESTAN
R552	The received signal covier level	+110	-90	NUMBER.
54R5 The visual representation of signal strength presented to the user. E.e. the number of bars on the daplay.		on the daploy. C	7	NUMBER.
GAIN The current transmitter gain setting.		-15	25	NUMBER.
POWER. The current power the phone is transmitting at.		-45	25	NUMBER.
SOCD	The delta number of glob frames which have occurred since the last reporting of this metric	0	255	NUMBER.
540	The deta number of error frames which have occurred since the last reporting of this metric	. c	255	NUMBER
	Rev OTA binery for this metric	-30	00	RAW
RAW BIN				

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).AndroidSecurityTest.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-o n-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-an droid-researcher/

(6). Russell Holly. Security researcher responds to CarrierIQ with video proof. http://www.geek.com/articles/mobile/security-researcher-responds-to-carrieriq-wit h-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-a pple-ios-iphone

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

(9). MSohm. Re: Does CarrierlQ run on BlackBerry devices?. http://supportforums.blackberry.com/t5/Java-Development/Does-CarrierlQ-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-eve r-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-me ssages-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.CarrierIQDetectorReleased.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.

Any technical information that is made available by Antiy Labs is the copyrighted work of Antiy Labs and is owned by Antiy Labs. NO WARRANTY. Antiy Labs makes no warranty as to this document's accuracy or use. The information in this document may include typographical errors or inaccuracies, and may not reflect the most current developments; and Antiy Labs does not represent, warrant or guarantee that it is complete, accurate, or up-to-date, nor does Antiy Labs offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Antiy Labs assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Antiy Labs reserves the right to make changes at any time without prior notice.

### **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 <u>www.antiy.net</u>.



Antiy Labs

Copyright ©2012 Antiy Labs. All rights reserved