TOP SECRET STRAP 2

NETWORK ANALYSIS CENTRE

Mobile Networks in

World

[redacted] Head of GCHQ NAC

TOP SECRET STRAP 2

What is a MyNOC ?

- MyNOC – My Network Operations Centre
  - A Space
  - A Concept

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

A Space

- Analyst Desktop X 10
- Un-attributable internet X 10
- JTRIG Desktop
- HIGHNOTE – CNE Toolsuite
- COPPERHEAD – CNE Attack box
- NEXUS (BSS Desktop)
- CADDIS (SIS Desktop)
- NRT Tipping Display
- 65” VTC/Collaborative Monitor and Projector
- Virtual Whiteboarding tool and Whiteboard
- Secure telpehony / storage

NAC
NETWORK ANALYSIS CENTRE

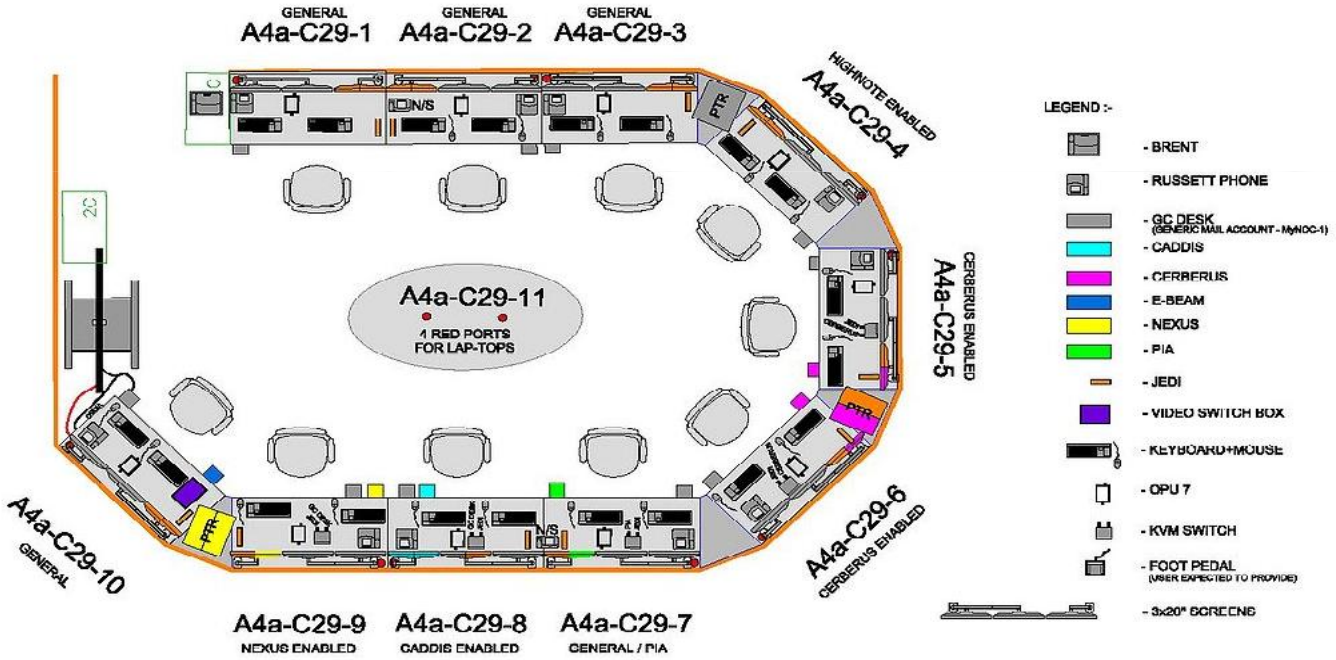
TOP SECRET STRAP 2

A Space

MyNoc Locations

The MyNocs are located as follows and contain the following capabilities;

- MyNOC1 A4a,
- MyNOC2 C4c,
- MyNOC3 B1d
- MyNOC4 C4d
- MyNOC5 A4f



NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

Interlopers in A Space

TOP SECRET STRAP 2

A Concept

- **Collaboration** environment bringing together capability from **across GCHQ**.
- Appropriate **resources** identified / Appropriate **prioritisation**
- Formalised planning process
  - Clear **Focused** objectives
  - Selection of **Operations Manager**
  - **Preparation**
  - Review
- Assessment and feasibility
- Professional Operations Manager
  - Ensure operation is focused on stated objectives
  - Ensures operation is legal
  - Protects information equities

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

MyNOC & NAC

- NAC tasked with development of “greater good” capability in Mobile/Mobile Internet environment.
- Due to lack of progress decision made to sponsor three MyNOC events:
  - OP WYLEKEY – Exploitation of International Mobile Billing Clearing Houses
  - OP SOCIALIST – Exploitation of GRX Operator
  - OP INTERACTION – Development of in-depth knowledge of Mobile Gateways.

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

MyNOC Team assemble

- Operations Manager
- Network Analysts (NAC Cheltenham, NAC Bude & NAC Cyprus)
- Dataminer (GTAC)
- Open Source Specialist
- JTRIG Analysts (Cheltenham & Bude)
- CNE Operators (Cheltenham CNE & Scarborough CNE)
- VPN Expert (Crypt SD)
- EREPO Expert (CNE)
- Protocol Analyst (GTE)
- Production Tasking Co-ordinator (PTC)
- Trainee Ops Managers

TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

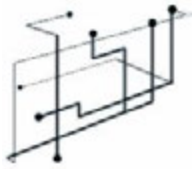
- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

Preparation work

- Identified static web gateways and IP range used by engineers and tasked for QUANTUM operations
- Identification and tasking of optimal bearers
- TDI data mining identified potential for exploitation of LinkedIn as a vector for QI – QI capability developed for LinkedIn
- WOODCUTTER logs analysed for usage by BELGACOM.



NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

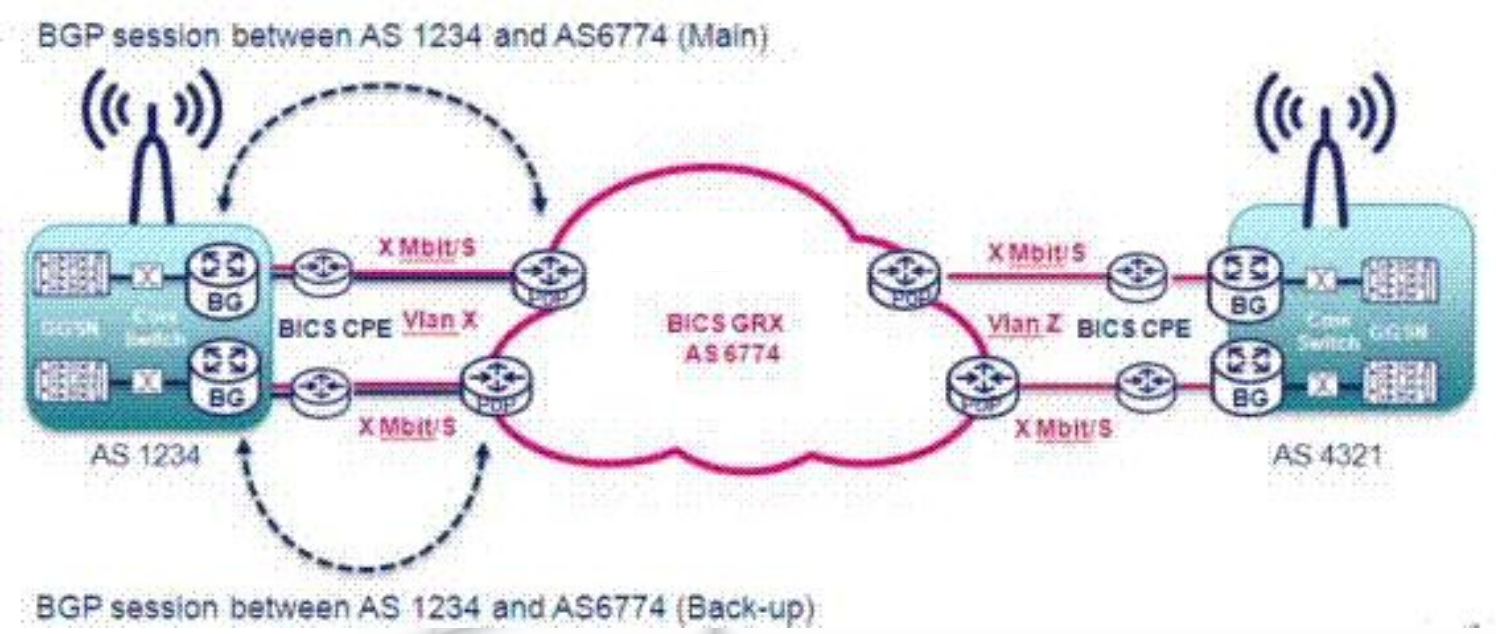
MyNOC Focus

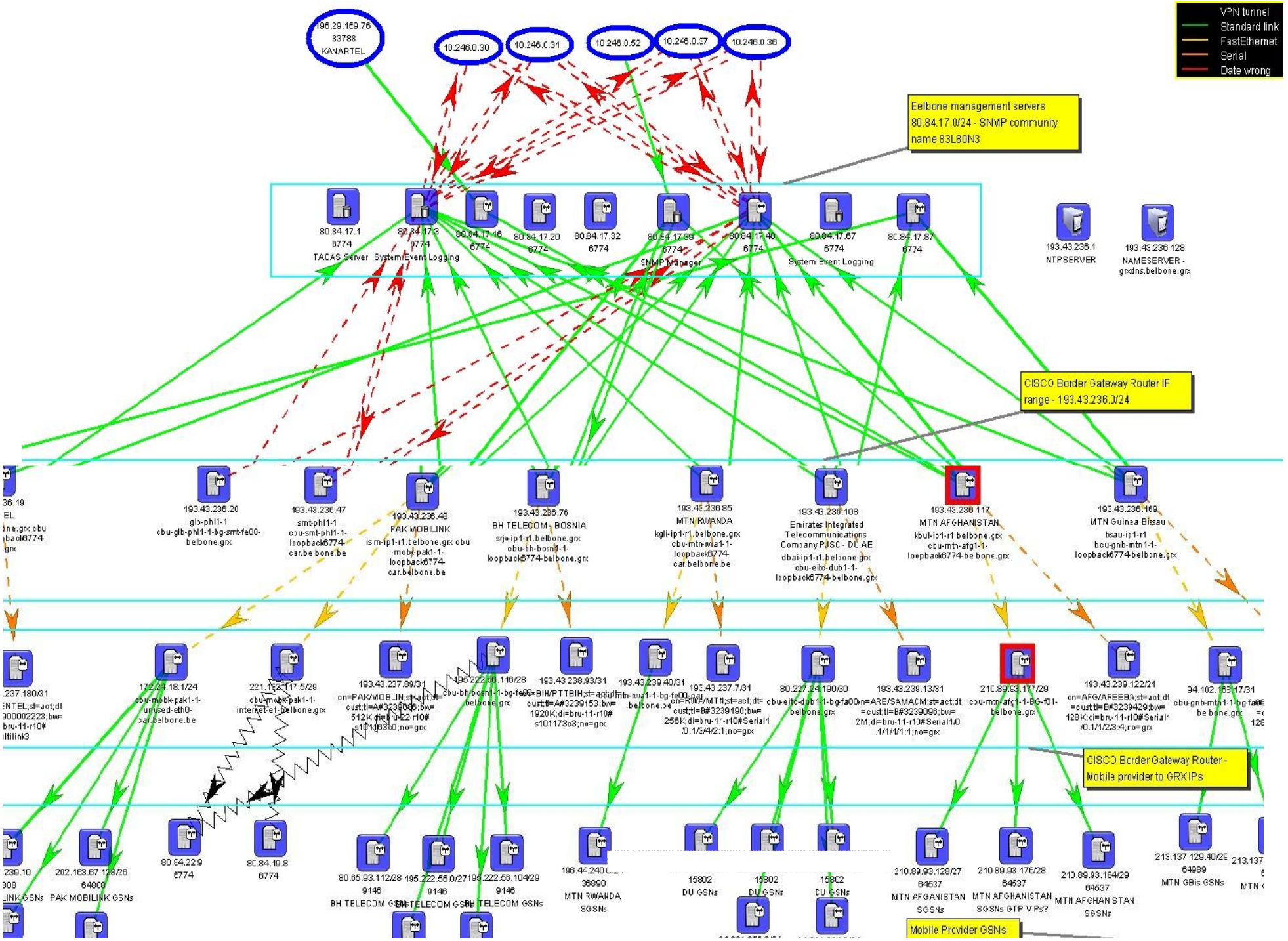
- Expand **collection and capability** to enable better exploitation of Belgacom.
- Identify **key staff at BICS**, and selectors used by these individuals for QI.
- **Map the network** to better understand the Belgacom Infrastructure.
- Investigate **VPN links** from BICS to other telecoms providers.
- Investigate the vulnerability of the **MyBICS** Reporting Tool.

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

Infrastructure




VPN tunnel
Standard link
FastEthernet
Serial
Date wrong
196.29.169.76
33788
KAVARTEL
10.246.0.30
10.246.0.31
10.246.0.52
10.246.0.37
10.246.0.36
Eelbone management servers
80.84.17.0/24 - SNMP community
name 83L80N3
80.84.17.1
6774
TACAS Server
80.84.17.173
6774
System Event Logging
80.84.17.46
6774
80.84.17.20
6774
80.84.17.32
6774
80.84.17.39
6774
SNMP Manager
80.84.17.40
6774
80.84.17.67
6774
System Even: Logging
80.84.17.87
6774
193.43.236.1
NTPSERVER
193.43.236.128
NAMESERVER -
gxdns.belbone.grx
CISCO Border Gateway Router IF
range - 193.43.236.0/24
193.43.236.20
glb-phl1-1
cbu-glb-phl1-1-bg-smt-fe00-
belbone.grx
193.43.236.47
smt-phl1-1
cbu-smt-phl1-1-
loopback6774-
car.belbone.be
193.43.236.48
PAK MOBILINK
ism-ip1-r1.belbone.grx cbu
-mobl-pak1-1-
loopback6774-
car.belbone.be
193.43.236.76
BH TELECOM - BOSNIA
srjw-ip1-r1.belbone.grx
cbu-bh-bosn1-1-
loopback6774-belbone.grx
193.43.236.85
MTN RWANDA
kgli-ip1-r1.belbone.grx
cbu-mtn-rwa1-1-
loopback6774-
car.belbone.be
193.43.236.108
Emirates Integrated
Telecommunications
Company PJSC - DU AE
dbai-ip1-r1.belbone.grx
cbu-eitc-dub1-1-
loopback6774-belbone.grx
193.43.236.117
MTN AFGHANISTAN
kbul-ip1-r1.belbone.grx
cbu-mtn-afg1-1-
loopback6774-belbone.grx
193.43.236.169
MTN Guinea Bissau
bsau-ip1-r1
cbu-gnb-mtn1-1-
loopback6774-belbone.grx
172.24.18.1/24
cbu-mobk-pak1-1-
unused-eth0-
car.belbone.be
221.132.117.5/29
cbu-mobk-pak1-1-
internet-e1-belbone.grx
193.43.237.89/31
cn=PAK/MOBILIN;st=act;dt=
cust;tl=A#3239063;bw=
512K;di=bru-22-r10#
s101163c0;no=grx
195.222.56.116/28
cbu-bh-bosn1-1-bg-fe00-
belbone.grx
193.43.238.93/31
cn=BIH/PTTBIH;st=act;dt=
cust;tl=A#3239153;bw=
1920K;di=bru-11-r10#
s101173c3;no=grx
193.43.239.40/31
cn=RWA/MTN;st=act;dt=
cust;tl=B#3239190;bw=
256K;di=bru-11-r10#Serial1
/0.1/3/4/2:1;no=grx
193.43.237.7/31
cbu-eitc-dub1-1-bg-fa00-
belbone.grx
193.43.239.13/31
cn=ARE/SAMACM;st=act;dt
=cust;tl=B#3239096;bw=
2M;di=bru-11-r10#Serial1/0
/1/1/1/1:1;no=grx
210.89.93.177/29
cbu-mtn-afg1-1-bg-fe01-
belbone.grx
193.43.239.122/21
cn=AFG/AFEEBA;st=act;dt
=cust;tl=B#3239429;bw=
128K;ci=bru-11-r10#Serial
/0.1/1/2/3:4;no=grx
CISCO Border Gateway Router -
Mobile provider to GRX IPs
202.163.67.128/26
64808
PAK MOBILINK GSNs
80.64.22.9
6774
80.84.19.8
6774
80.65.93.112/28
9146
BH TELECOM GSNs
195.222.56.0/27
9146
BH TELECOM GSNs
195.222.56.104/29
9146
BH TELECOM GSNs
196.44.240.0/24
36890
MTN RWANDA
SGSNs
15802
DU GSNs
15802
DU GSNs
15802
DU GSNs
210.89.93.128/27
64537
MTN AFGANISTAN
SGSNs
210.89.93.176/28
64537
MTN AFGHANISTAN
SGSNs GTP VPs?
210.89.93.184/29
64537
MTN AFGHAN STAN
SGSNs
213.137.129.40/29
64989
MTN GBis GSNs
Mobile Prcvider GSNs

TOP SECRET STRAP 2

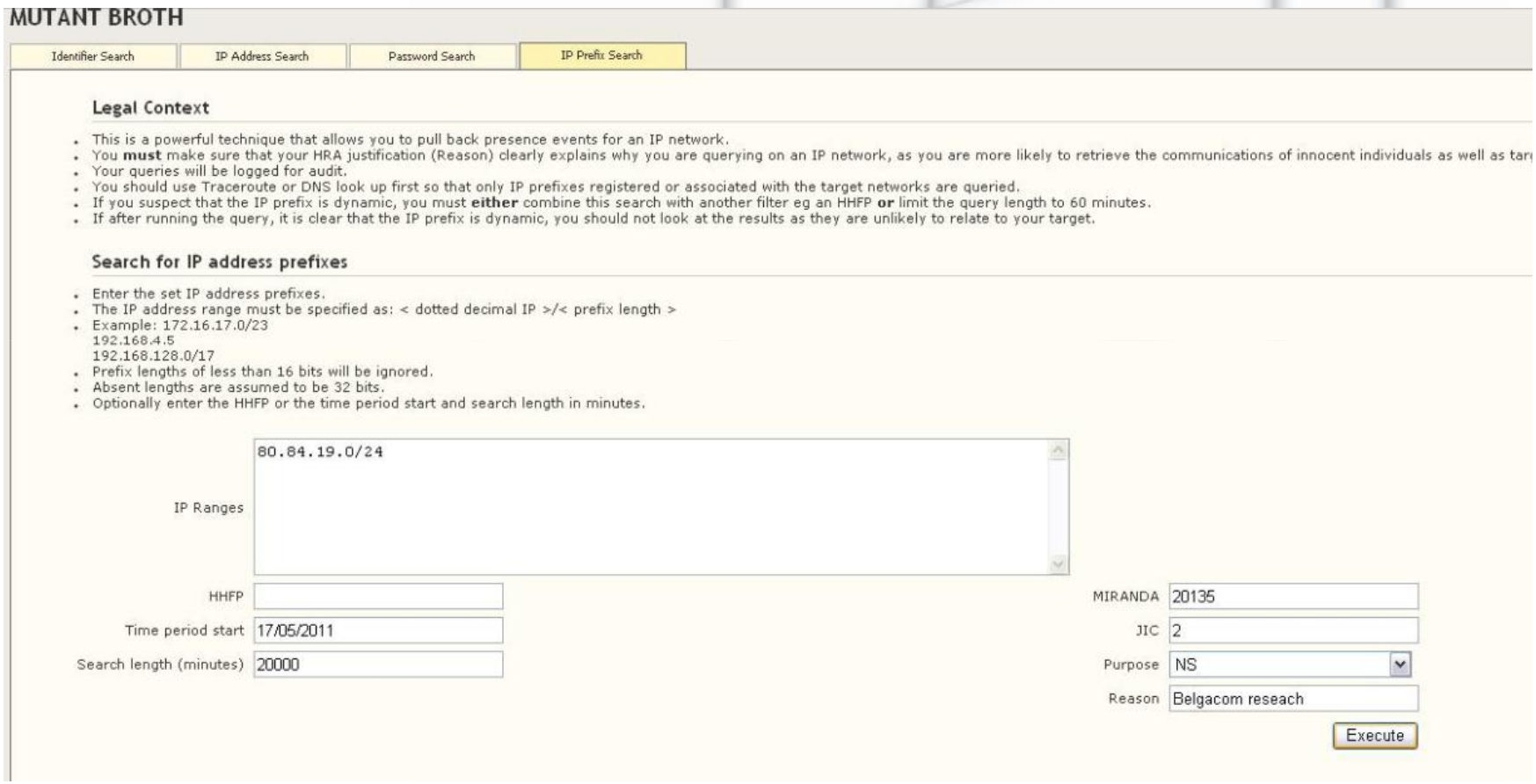
Key BELGACOM staff

- Identify Belgacom employees
  - NOC staff
  - In areas related to maintenance or security
- Selectors to enable QUANTUM targeting
  - Use of LinkedIn noted
  - Use of Slashdot.org noted
- MUTANT BROTH used to identify TDI/Selectors coming from identified range/proxy
- QI capability enhanced to allow shots on LinkedIn
- QI capability enhanced to allow ‘white listing’ when shooting on proxy

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

NOC IP range search in MUTANT BROTH



TOP SECRET STRAP 2

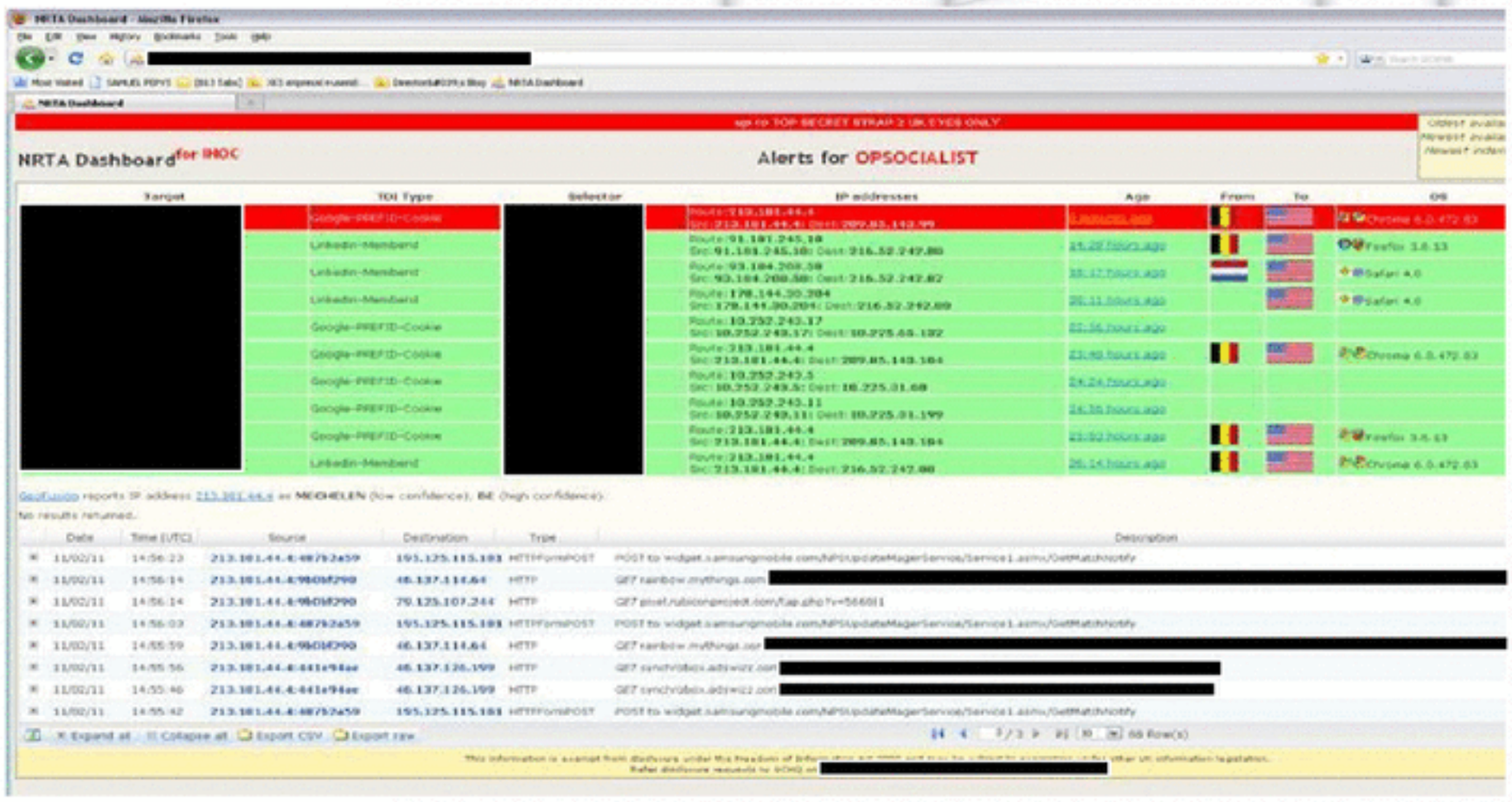
NOC IP range – Target identifiers for QUANTUM INSERT

Source IP	User-Agent	Date	Time	Non Routine Source	Source IP:HHFP	Source IP Geo	Identifier Type	Identifier Value	Event Count (%)
80.84.19.9									
	Mozilla/5.0 (X								(4 %)
	Mozilla/5.0 (X	17/05/11	00:02:54		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LLM	Yahoo-B-Cookie	[redacted]	(4 %)
	Mozilla/5.0 (X								(2 %)
	Mozilla/5.0 (X	17/05/11	00:02:59		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LLM	Yahoo-B-Cookie		(0 %)
	Mozilla/4.0 (c								(1 %)
	Mozilla/5.0 (X	17/05/11	00:02:59		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LHV	Yahoo-B-Cookie		6 (16 %)
	Mozilla/5.0 (W								(4 %)
	Mozilla/5.0 (X	17/05/11	00:05:37		80.84.19.9:5eec974d	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		2 (14 %)
	Mozilla/5.0								(0 %)
	Mozilla/5.0 (X	17/05/11	00:16:18		80.84.19.9:7d9134a5	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		4 (28 %)
	Mozilla/5.0 (X								2 (18 %)
	Mozilla/5.0 (W	17/05/11	00:17:58		80.84.19.9:77387b02	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		(3 %)
		17/05/11	00:23:35		80.84.19.9:e4a90e3f	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:28:05		80.84.19.9:7d9134a5	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:37:34		80.84.19.9:b36815d3	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:39:55		80.84.19.9:f12897e0	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:47:56		80.84.19.9:477c4721	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:54:38		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-		

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

Real-time picture of QI



NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

GTAC effort

- IR21 extractions
- Website research – domains visited from target gateway IPs
- TDI harvesting
- Identified owners of TDIs / finding new potential targets
- Identified the FTP service
- User agent analysis
- Laptop identification
- Mail server analysis
- SSL research
- GRX analysis

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

What MyNOC Priority gets you

- Dedicated resources
- Priority tasking of access
- Priority utilisation of CNE Operator resources
- Priority utilisation of CNE Developer resources
- Priority use of enabling community (GTE, GTAC, JTRIG)
- Priority time of legalities bodies

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

OP SOCIALIST Outcome

- In MyNOC:
  - CNE Access to BELGACOM – MERION ZETA – 6 endpoints into Engineer/support staff IP range
  - 2 endpoints into BELGACOM DMZ (from prep VA work)
  - Optimal Bearers identified providing good access to BELGACOM proxy.
- Post MyNOC:
  - Optimal Bearers continue to allow QI against BELGACOM engineers/proxy
  - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on hosts with access
  - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

TOP SECRET STRAP 2

MyNOC leave behinds for NAC

- Focused working in small groups
- Regular Brainstorming sessions
- Professional Operational Management
- Network becomes Target – Target approach to Network Problems
- Awareness of JTRIG and Open-source information specialist capabilities and how they can support Network Analysis.
- Steerage of access for Network Analysis gain
- Closer working between NAC and CNE
- Joint working between NACs
- More NAC MyNOC/Focus efforts to come….

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2

Questions ?