NETWORK ANALYSIS CENTRE

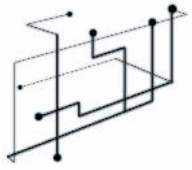
# Automated NOC Detection

[redacted], Head of GCHQ NAC

[redacted], Senior Network Analyst, CSEC NAC

# Challenge

- SDC 2009 – Challenged the Network Analysis community to automate the detection of Network Operations Centres

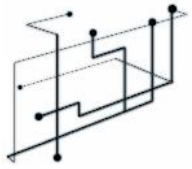


NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## Phase 1: Intelligent Router Configuration File Parsing

- Routers have numerous services running on them that help identify the NOC IP ranges:
  - SSH
  - TELNET/VTY
  - SNMP
  - SYSLOG
  - DNS
  - TACACS
  - RADIUS
- Access to these services tends to be locked down by the use of Access Control Lists (ACLs)
- Configuration files provide details of how services are configured.

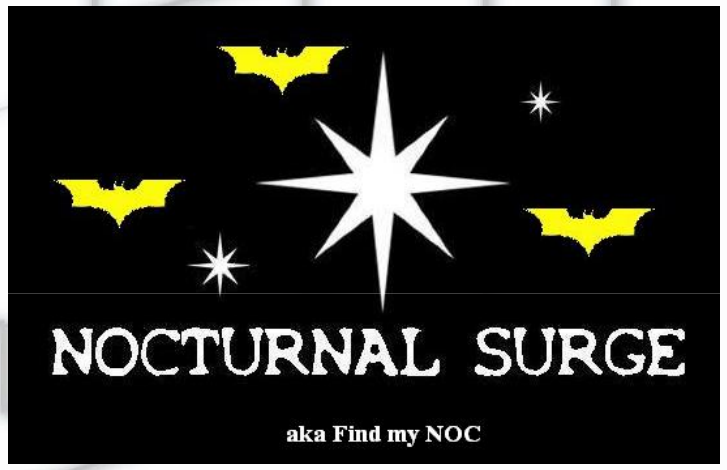


NETWORK ANALYSIS CENTRE

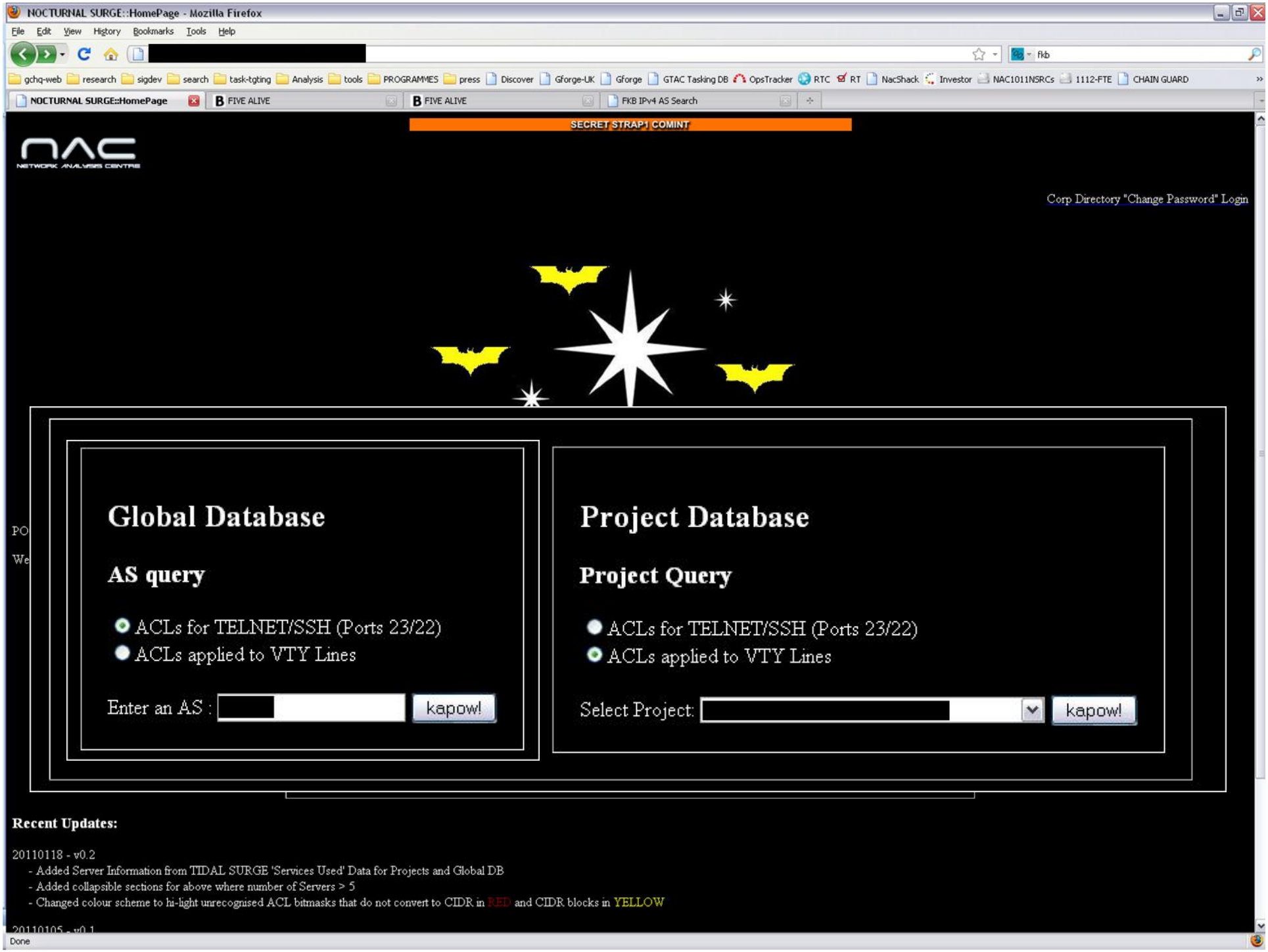
# TOP SECRET STRAP 2

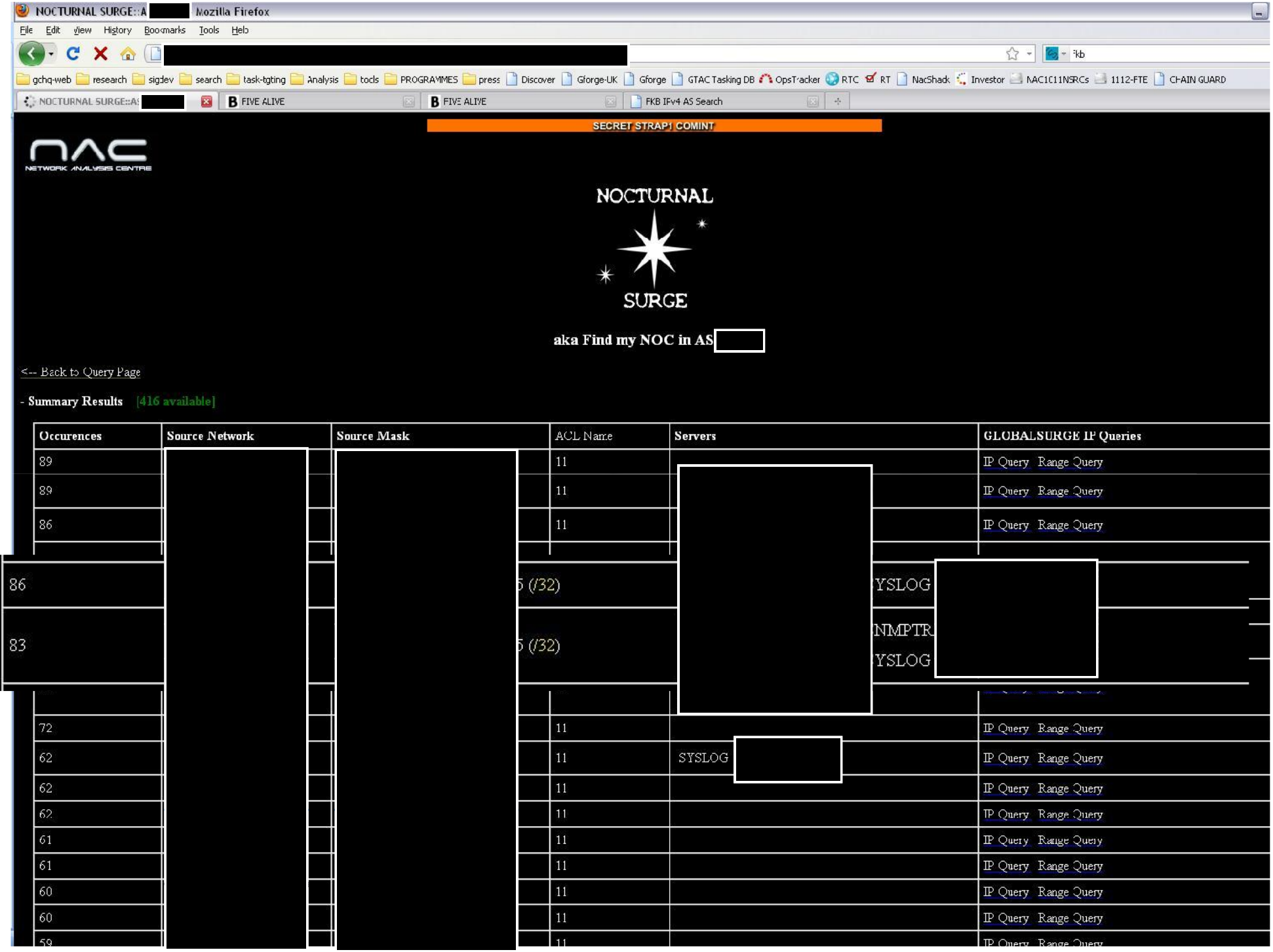
## NOCTURNAL SURGE

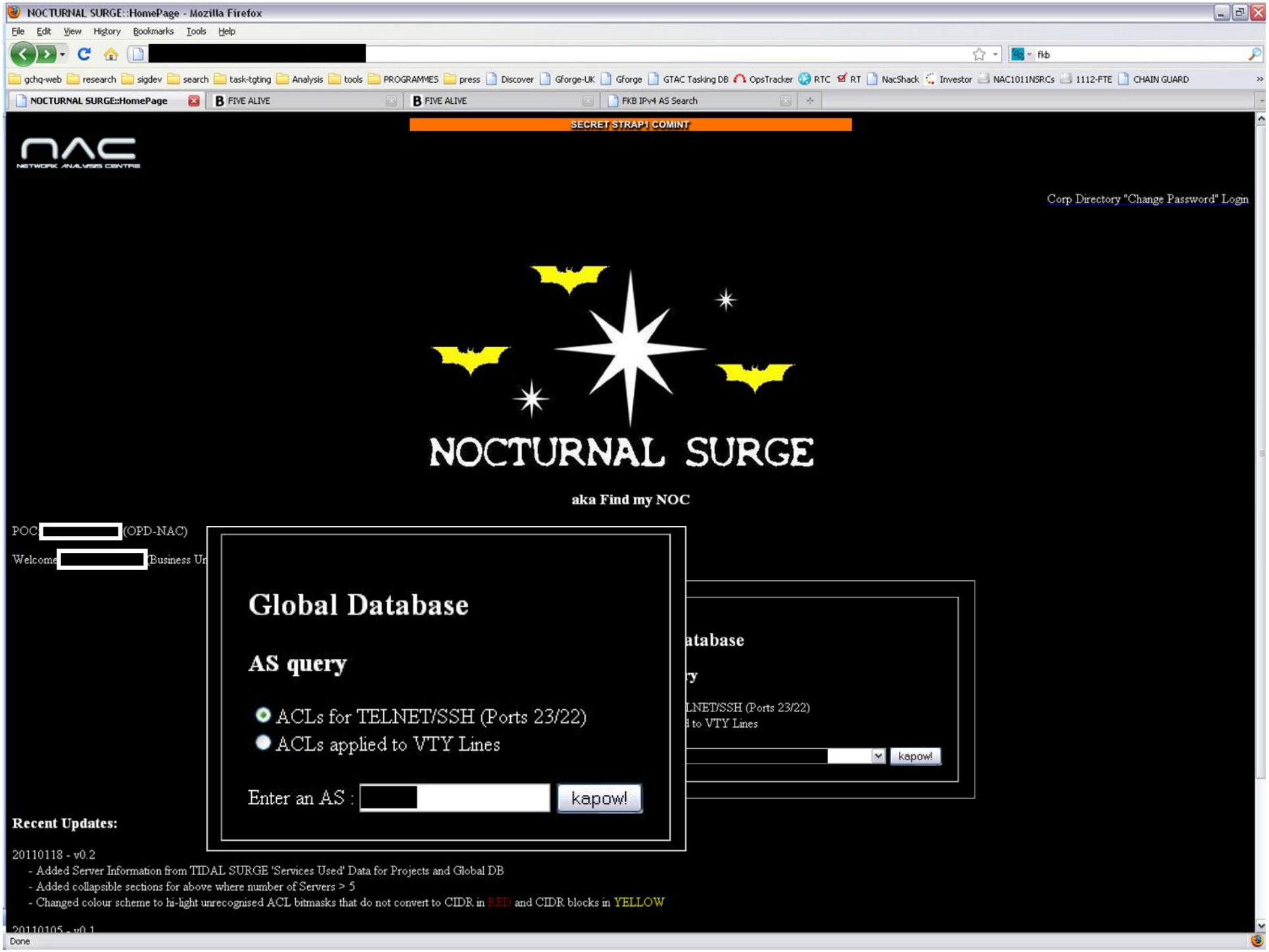
- GCHQ response to challenge.
- Early Prototype that looks at only:
  - ACLs for SSH/TELNET
  - ACLs for VTY

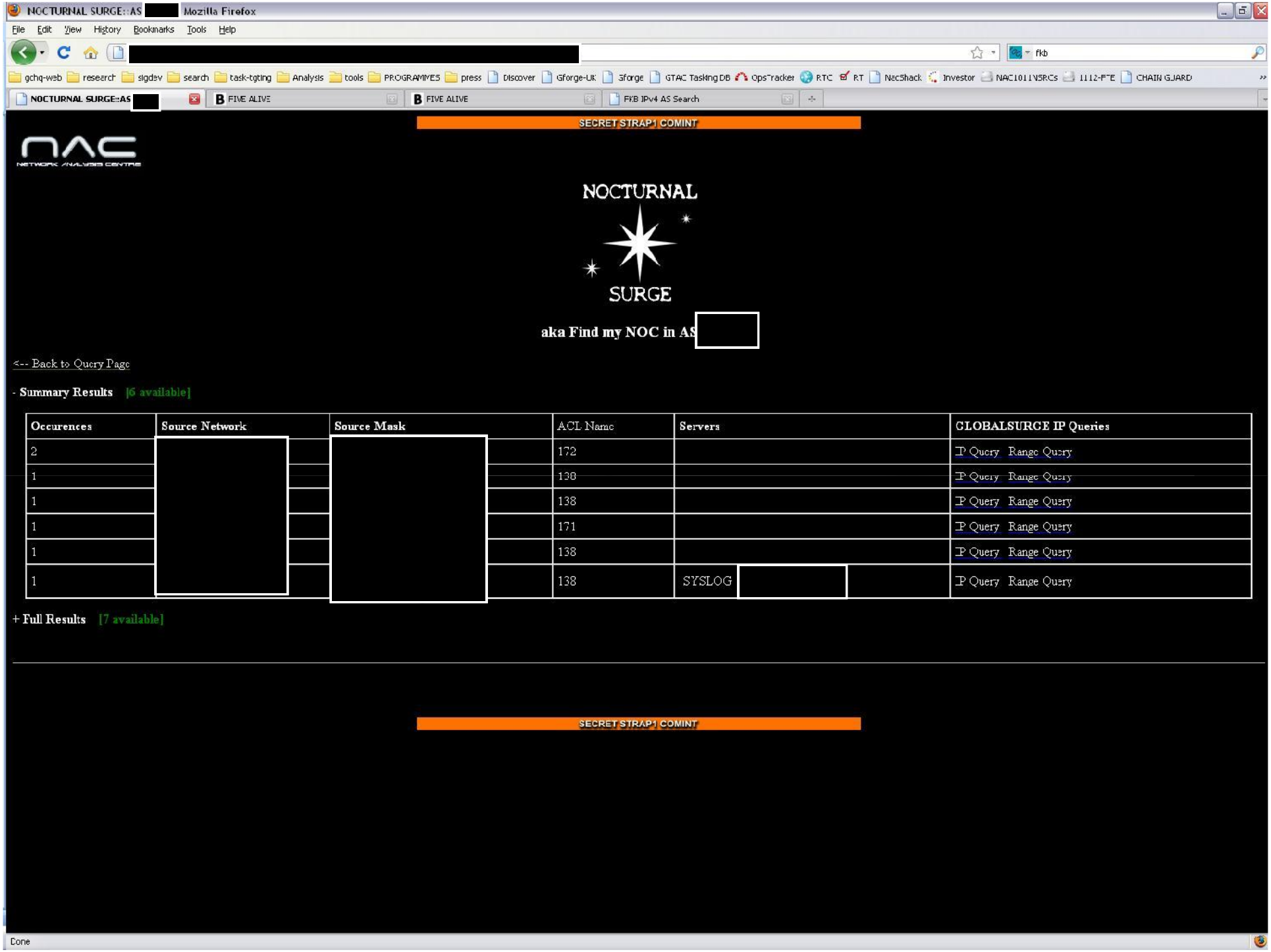



NETWORK ANALYSIS CENTRE


NOCTURNAL SURGE::HomePage - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NOCTURNAL SURGE::HomePage
FIVE ALIVE
FIVE ALIVE
FKB IPv4 AS Search
SECRET STRAP1 COMINT
NETWORK ANALYSIS CENTRE
Corp Directory "Change Password" Login
Global Database
AS query
ACLs for TELNET/SSH (Ports 23/22)
ACLs applied to VTY Lines
Enter an AS :
kapow!
Project Database
Project Query
ACLs for TELNET/SSH (Ports 23/22)
ACLs applied to VTY Lines
Select Project:
kapow!
Recent Updates:
20110118 - v0.2
- Added Server Information from TIDAL SURGE 'Services Used' Data for Projects and Global DB
- Added collapsible sections for above where number of Servers > 5
- Changed colour scheme to hi-light unrecognised ACL bitmasks that do not convert to CIDR in RED and CIDR blocks in YELLOW
Done


NOCTURNAL SURGE::A [redacted] Mozilla Firefox
File Edit View History Bookmarks Tools Help
gchq-web research sigdev search task-tgting Analysis tools PROGRAMMES press Discover Gforge-UK Gforge GTAC Tasking DB OpsTracker RTC RT NacShack Investor NAC1C11NSRCs 1112-FTE CHAIN GUARD
NOCTURNAL SURGE::A[redacted]
FIVE ALIVE
FIVE ALIVE
FKB IPv4 AS Search
SECRET STRAP1 COMINT
NAC
NETWORK ANALYSIS CENTRE
NOCTURNAL
SURGE
aka Find my NOC in AS[redacted]
<-- Back to Query Page
- Summary Results [416 available]
Occurences
Source Network
Source Mask
ACL Name
Servers
GLOBALSURGE IP Queries
89 11 IP Query Range Query
89 11 IP Query Range Query
86 11 IP Query Range Query
86 5 (32) YSLOG
83 5 (32) NMPTR YSLOG
72 11 IP Query Range Query
62 11 SYSLOG IP Query Range Query
62 11 IP Query Range Query
62 11 IP Query Range Query
61 11 IP Query Range Query
61 11 IP Query Range Query
60 11 IP Query Range Query
60 11 IP Query Range Query
59 11 IP Query Range Query

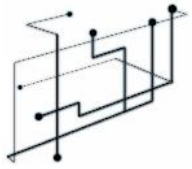

NOCTURNAL SURGE::HomePage - Mozilla Firefox
File Edit View History Bookmarks Tools Help
NOCTURNAL SURGE::HomePage
FIVE ALIVE
FIVE ALIVE
FKB IPv4 AS Search
SECRET STRAP1 COMINT
NETWORK ANALYSIS CENTRE
Corp Directory "Change Password" Login
NOCTURNAL SURGE
aka Find my NOC
POC (OPD-NAC)
Welcome (Business Ur
Global Database
AS query
ACLs for TELNET/SSH (Ports 23/22)
ACLs applied to VTY Lines
Enter an AS :
kapow!
Recent Updates:
20110118 - v0.2
- Added Server Information from TIDAL SURGE 'Services Used' Data for Projects and Global DB
- Added collapsible sections for above where number of Servers > 5
- Changed colour scheme to hi-light unrecognised ACL bitmasks that do not convert to CIDR in RED and CIDR blocks in YELLOW
Done


NOCTURNAL SURGE::AS [redacted] Mozilla Firefox
File Edit View History Bookmarks Tools Help
[redacted]
fkb
gchq-web research sigdev search task-tgting Analysis tools PROGRAMMES press Discover GForge-UK GForge GTAC Tasking DB OpsTracker RTC RT NecShack Investor NAC1011N5RCs 1112-F5E CHAIN GJARD
NOCTURNAL SURGE::AS [redacted]
FIVE ALIVE
FIVE ALIVE
FKB IPv4 AS Search
SECRET STRAP1 COMINT
NETWORK ANALYSIS CENTRE
NOCTURNAL
SURGE
aka Find my NOC in AS [redacted]
<-- Back to Query Page
- Summary Results [6 available]
Occurences
Source Network
Source Mask
ACL Name
Servers
GLOBALSURGE IP Queries
2 [redacted] [redacted] 172 IP Query Range Query
1 138 IP Query Range Query
1 138 IP Query Range Query
1 171 IP Query Range Query
1 138 IP Query Range Query
1 138 SYSLOG [redacted] IP Query Range Query
+ Full Results [7 available]
SECRET STRAP1 COMINT
Done

# TOP SECRET STRAP 2

## GCHQ / CSEC NAC Joint tradecraft development

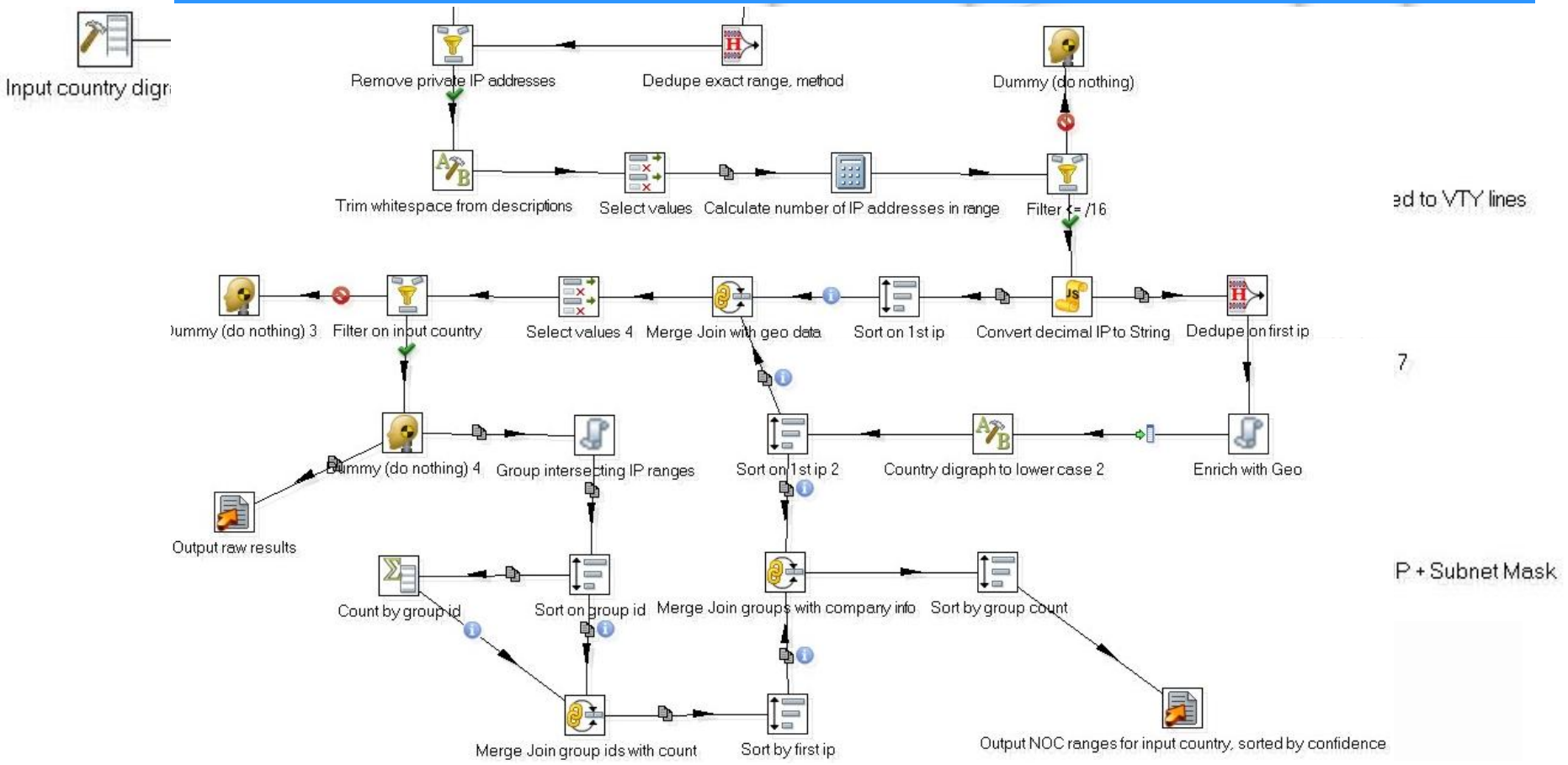
- During March 2011 GCHQ Analysts visited CSEC to look at the using PENTAHO for tradecraft modelling working with CSEC NAC and CSEC/H3 software developers to see if could model NOCTURNAL SURGE in PENTAHO and then implement in OLYMPIA.
- Only possible to attempt because:
  - GCHQ NAC use PENTAHO
  - CSEC NAC/H3 use PENTAHO
  - CSEC NAC have implemented GCHQ NAC TIDAL SURGE Database Schema (DSD also have this..)
- GCHQ approach based on AS
- CSEC approach based on Country



NAC
NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

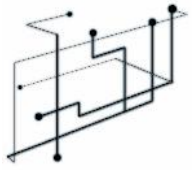
## Pentaho - NOC Auto Detection



# TOP SECRET STRAP 2

## Phase 2: Intelligent use of Metadata

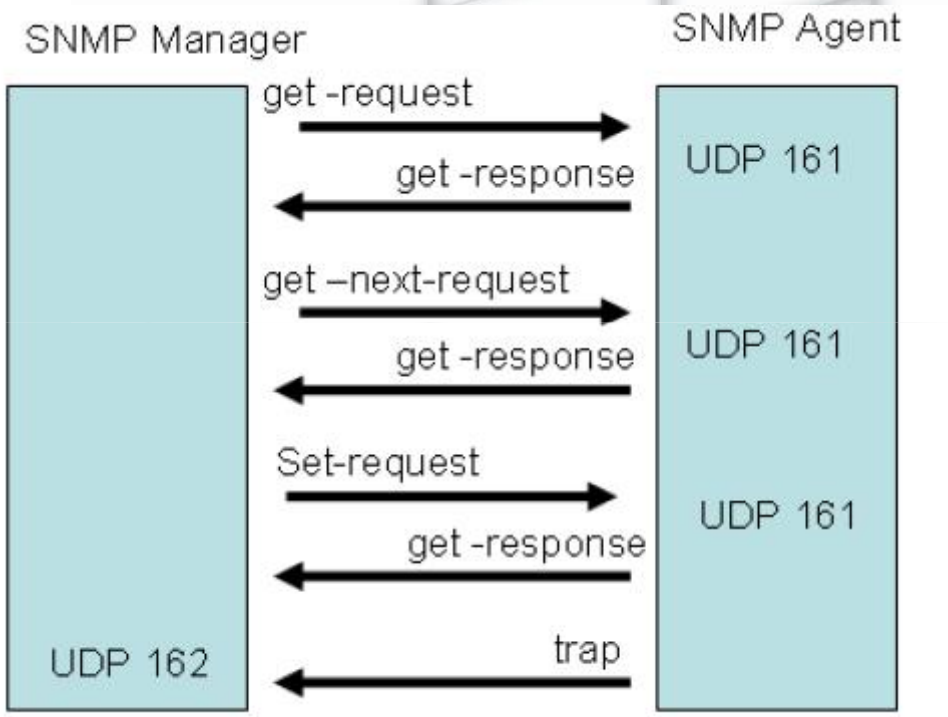
- We do not always get full configuration files to parse.
- Services between routers and NOCs run on IP/TCP/UDP
- We do create 5-TUPLE metadata from our collection
  - GCHQ have prototype database – 5-Alive
  - CSEC have database - HYPERION



NETWORK ANALYSIS CENTRE

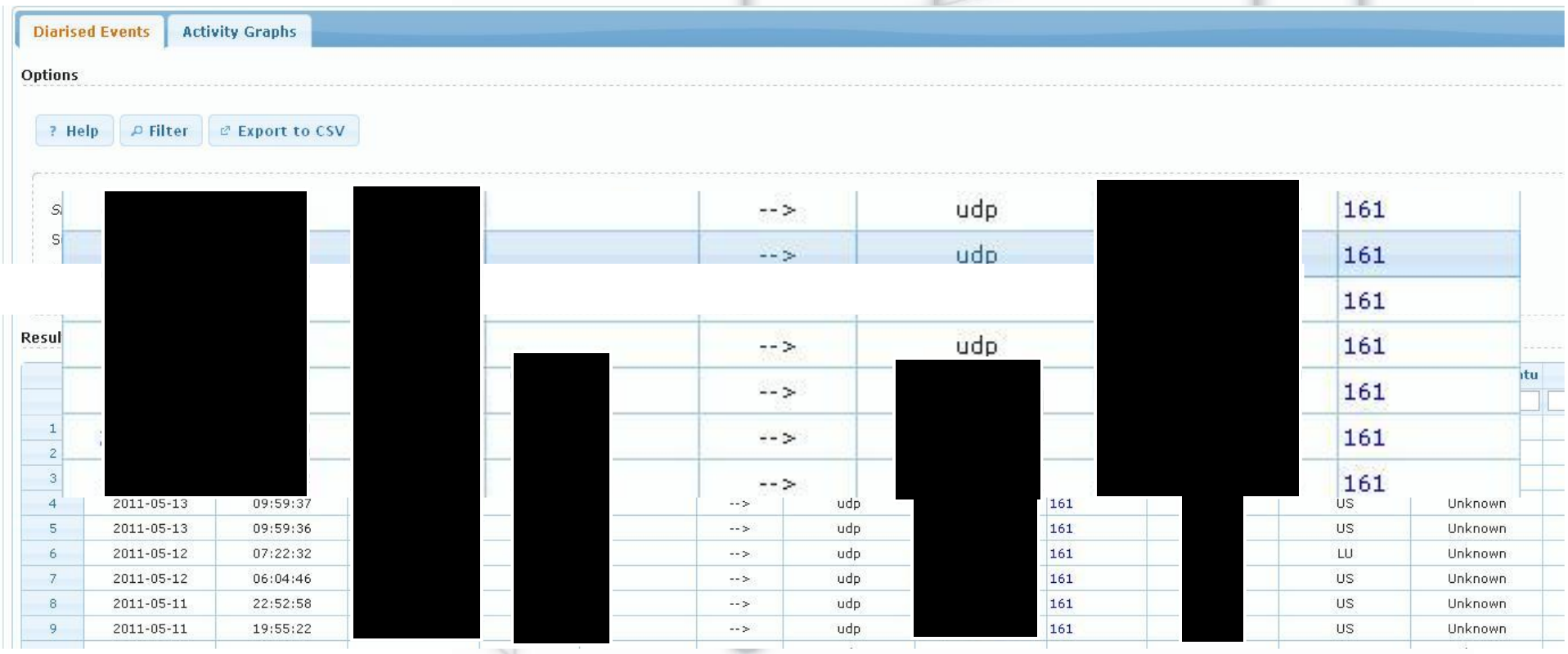
# TOP SECRET STRAP 2

## SNMP Protocol



# TOP SECRET STRAP 2

## SNMP Protocol in 5-Alive




NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

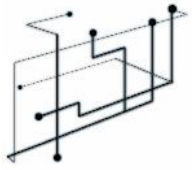
## Further drill down on activity for identified IP

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 20 | [redacted] | 17 | udp | | DNS (Domain Name System) | 63226 | 53 | 2011-05-12 | 07:30:00 | 2011-05-12 | 08:00:00 |
| 21 | | 17 | udp | | Trivial File Transfer Protocol TFTP | 52096 | 69 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 22 | | 17 | udp | | Trivial File Transfer Protocol TFTP | 58912 | 69 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 23 | | 17 | udp | | Trivial File Transfer Protocol TFTP | 53438 | 69 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 24 | | 17 | udp | | Network Time Protocol NTP | 52096 | 123 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 25 | | 17 | udp | | Network Time Protocol NTP | 58912 | 123 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 26 | | 17 | udp | | Network Time Protocol NTP | 53438 | 123 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 27 | | 17 | udp | | NetBIOS NetBIOS Datagram Service | 53438 | 138 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 28 | | 17 | udp | | NetBIOS NetBIOS Datagram Service | 58912 | 138 | 2011-05-13 | 10:15:00 | 2011-05-13 | 10:45:00 |
| 29 | | 17 | udp | | NetBIOS NetBIOS Datagram Service | 52096 | 138 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |
| 30 | | 17 | udp | | Simple Network Management Protocol SNMP | 52096 | 161 | 2011-05-13 | 10:00:00 | 2011-05-13 | 10:30:00 |

# TOP SECRET STRAP 2

## Phase 3: Intelligent use of TELNET traffic

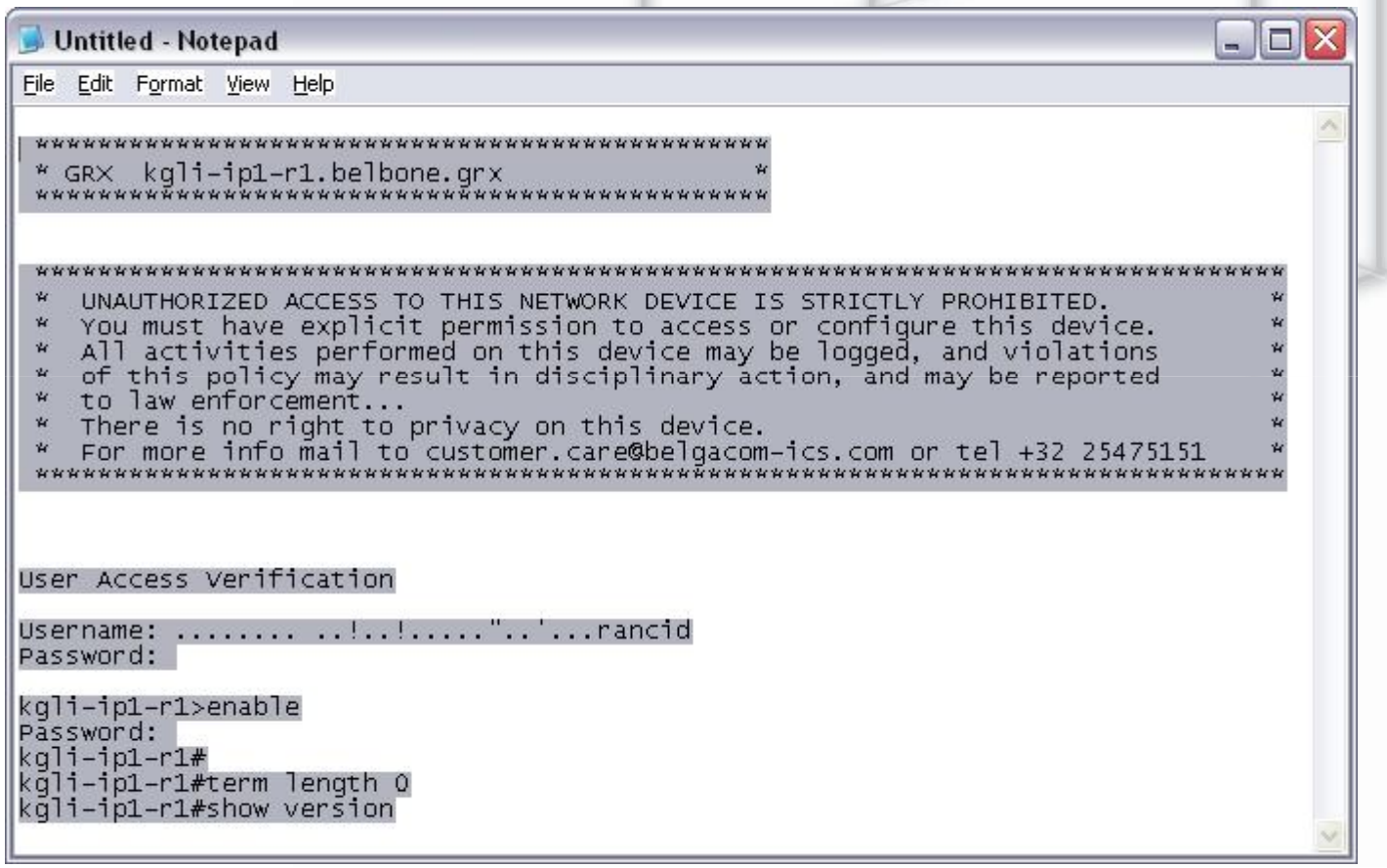
- Again we do not always get full configuration files. Phase 1 is based on full (or as near to full) configuration files
- GCHQ NAC collect TELNET Sessions into TERMINAL SURGE
  - Collection based on TCP Port 23 (TELNET)
  - Other protocols use TCP Port 23 (YMSG)
- Interaction with Routers over TCP Port 23 maybe nefarious:
  - Scanning
  - Password guessing
- Need to separate legitimate use from nefarious activity
- Look for signs of legitimate use.
  - Successful login
  - Follow on commands



NAC
NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

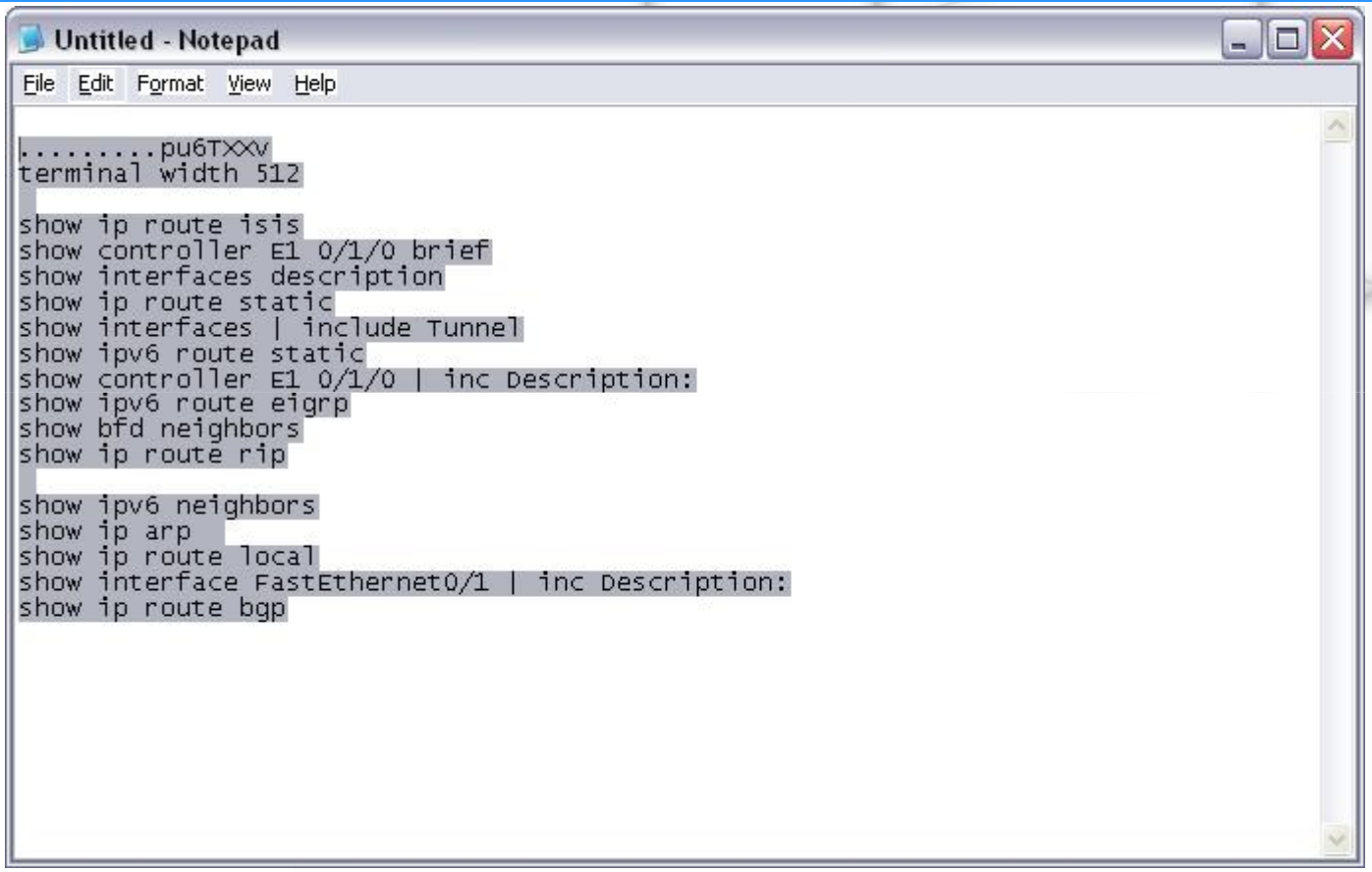
## From TCP Port 23 (Echo)




NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## To TCP Port 23



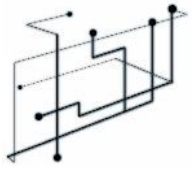
# TOP SECRET STRAP 2

## Intelligent analysis of TELNET traffic

- The fact that login was successful for both examples means the following:
  - From TCP Port 23
    - To IP address is Network Management Terminal (in the NOC ?)
  - To TCP Port 23
    - From IP address is Network Management Terminal (in the NOC ?)

# Phase 4: Bulk Port Scanning

- We know the key services/servers running in the NOC
- Utilise HACIENDA, GCHQ's bulk port scanning capability to identify what IPs have these service ports open – additional logic to build up confidence required.

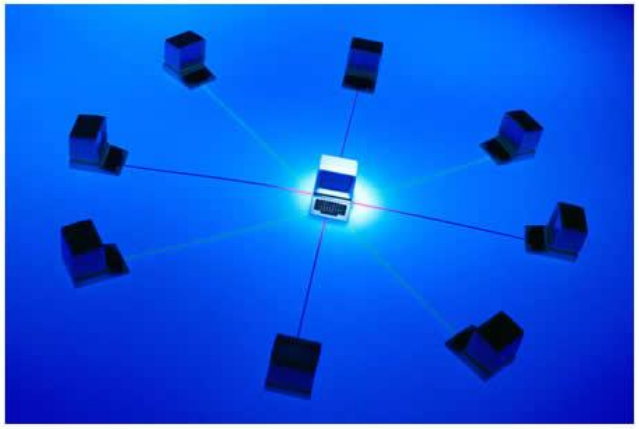


NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## Fusion of sources

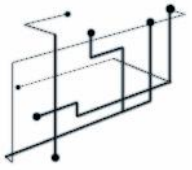
- Aim is to bring all sources that help identify NOC IP ranges together with associated confidence.
- Different techniques provide different results due to the nature of passive access (international v's in-country for instance)
- Different techniques have different levels of reliability – therefore looking to develop aggregation with overlay of smart intelligence.
- Solution can work on not just ISP NOCs but also Mobile OMCs.



# TOP SECRET STRAP 2

## And then….enabling CNE on NOCs

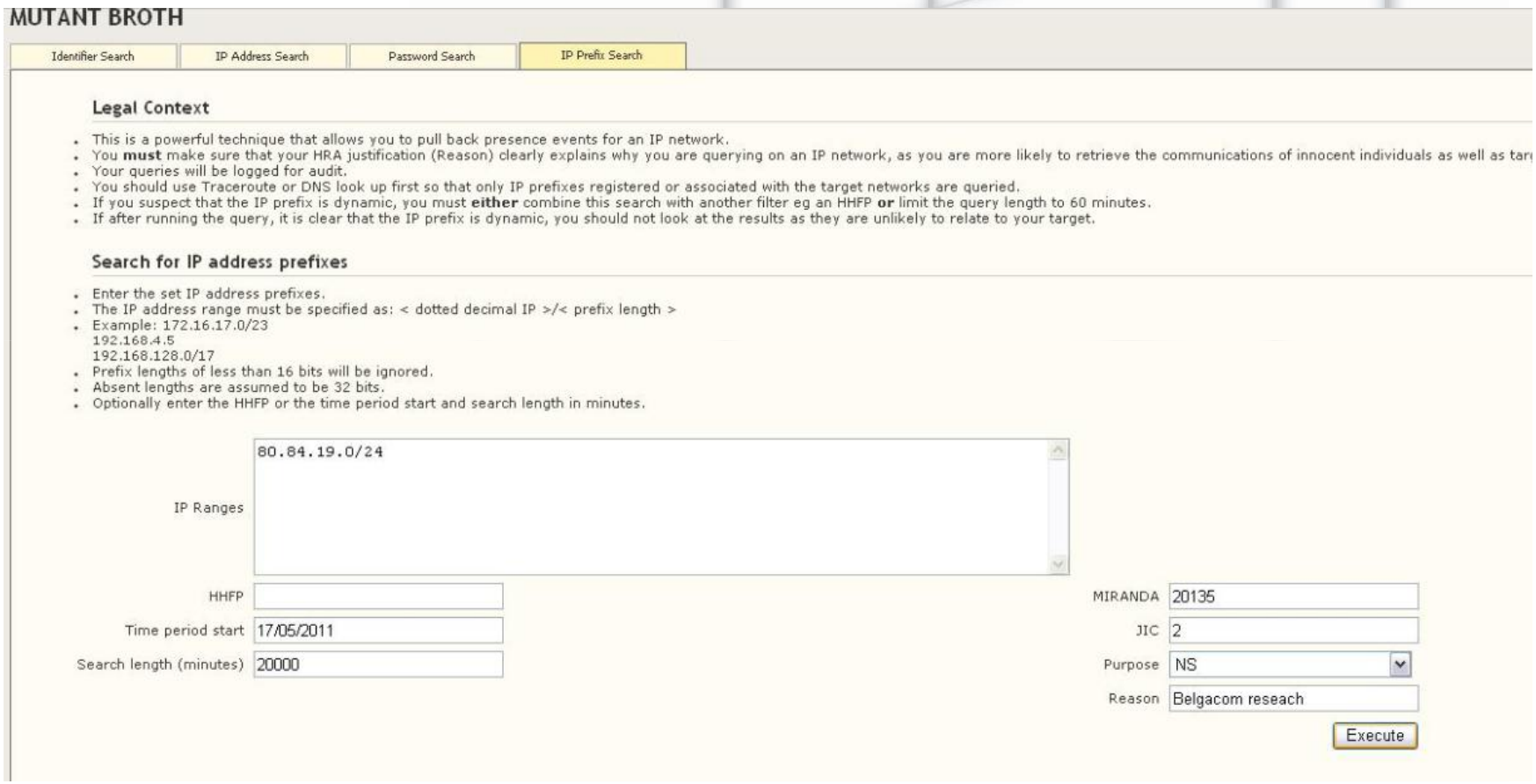
- We now have IP ranges – need selectors of NOC Staff to enable QUANTUM INSERT attack against them.
- Use of GCHQ TDI capability to identify selectors coming out of IP ranges and/or identification of proxy/NAT within NOC range.



NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## NOC IP range search in MUTANT BROTH

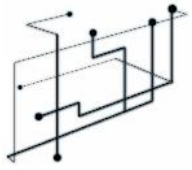



NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## NOC IP range – Target identifiers for QUANTUM INSERT

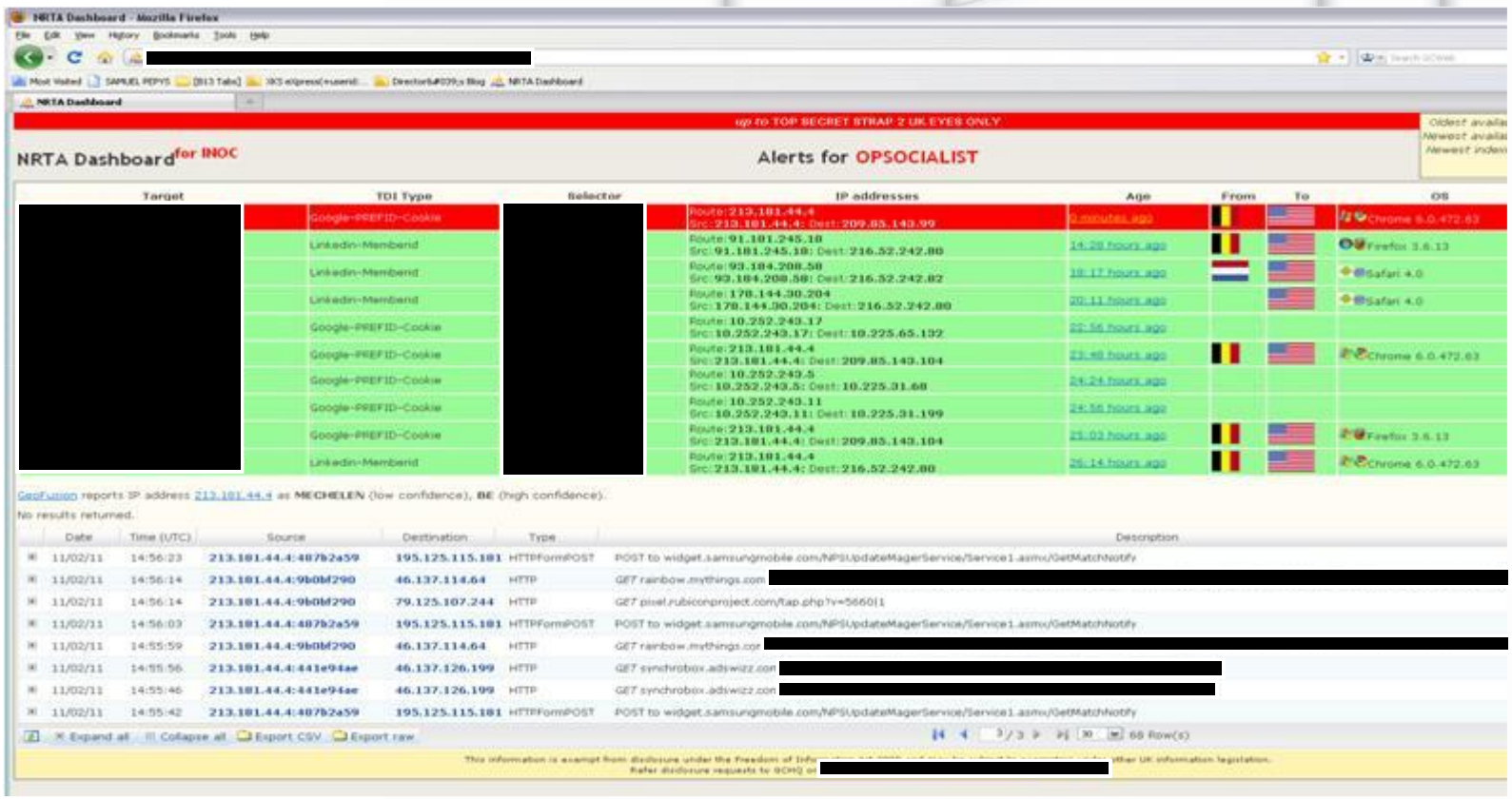
| Source IP | User-Agent | Date | Time | Non Routine Source | Source IP:HHFP | Source IP Geo | Identifier Type | Identifier Value | Event Count (%) |
|---|---|---|---|---|---|---|---|---|---|
| 80.84.19.9 | | | | | | | | | |
| | Mozilla/5.0 (X | | | | | | | | (4 %) |
| | Mozilla/5.0 (X | 17/05/11 | 00:02:54 | | 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- | | |



NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## Real-time picture of QI




NETWORK ANALYSIS CENTRE

# TOP SECRET STRAP 2

## Questions ?


NETWORK ANALYSIS CENTRE