

TOP SECRET STRAP 2

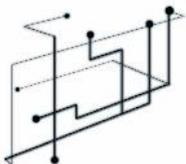


Automated NOC Detection



[REDACTED], Head of GCHQ NAC

[REDACTED], Senior Network Analyst, CSEC NAC

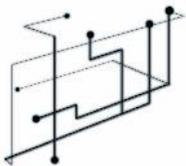


This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or [REDACTED]

TOP SECRET STRAP 2

Challenge

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



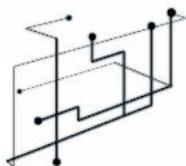
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or [REDACTED]

TOP SECRET STRAP 2

Phase 1: Intelligent Router Configuration File Parsing

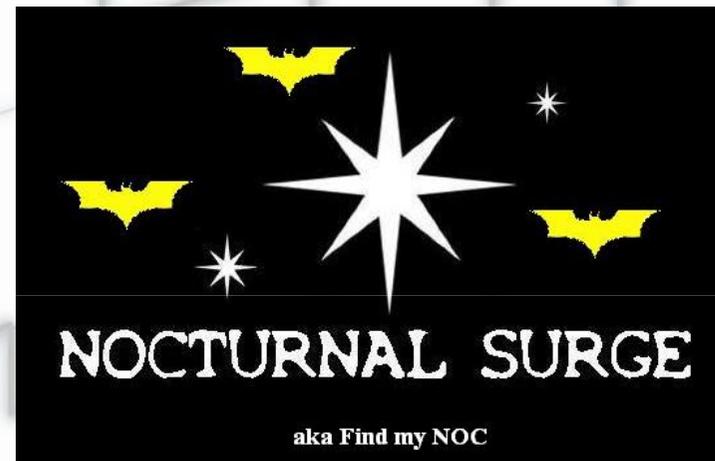
- Routers have numerous services running on them that help identify the NOC IP ranges:
 - SSH
 - TELNET/VTY
 - SNMP
 - SYSLOG
 - DNS
 - TACACS
 - RADIUS
- Access to these services tends to be locked down by the use of Access Control Lists (ACLs)
- Configuration files provide details of how services are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



TOP SECRET STRAP 2

NOCTURNAL SURGE

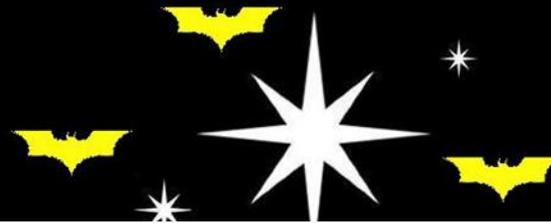
- GCHQ response to challenge.
- Early Prototype that looks at only:
 - ACLs for SSH/TELNET
 - ACLs for VTY



SECRET STRAP1 COMINT



Corp Directory "Change Password" Login



Global Database

AS query

- ACLs for TELNET/SSH (Ports 23/22)
- ACLs applied to VTY Lines

Enter an AS :

Project Database

Project Query

- ACLs for TELNET/SSH (Ports 23/22)
- ACLs applied to VTY Lines

Select Project:

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

20110105 - v0.1

Done

SECRET STRAP1 COMINT



NOCTURNAL



SURGE

aka Find my NOC in AS

<-- 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)		IP Query Range Query
83			5 (/32)		IP Query Range Query
					IP Query Range Query
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

SECRET STRAP1 COMINT



Corp Directory "Change Password" Login



NOCTURNAL SURGE

aka Find my NOC

POC [redacted] (OPD-NAC)
Welcome [redacted] Business Ur

Global Database

AS query

- ACLs for TELNET/SSH (Ports 23/22)
- ACLs applied to VTY Lines

Enter an AS :

Global Database

AS query

- ACLs for TELNET/SSH (Ports 23/22)
- ACLs applied to VTY Lines

Enter an AS :

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
- 20110105 - v0.1

SECRET STRAP1 COMINT



NOCTURNAL



SURGE

aka Find my NOC in AS

[<-- Back to Query Page](#)

Summary Results [6 available]

Occurrences	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 <input type="text"/>

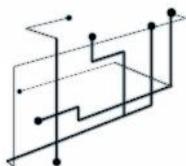
+ Full Results [7 available]

SECRET STRAP1 COMINT

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

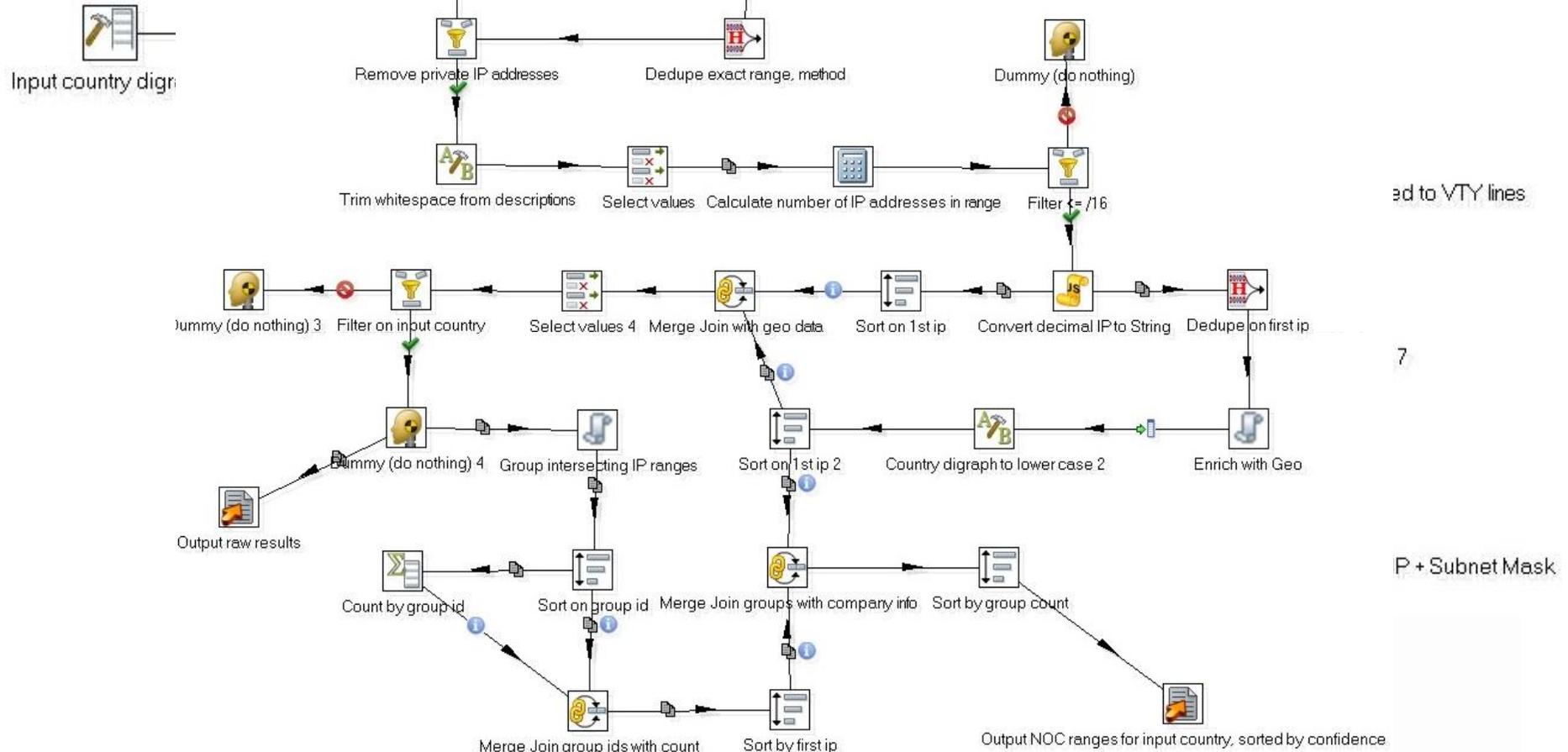


NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GC [REDACTED]

TOP SECRET STRAP 2

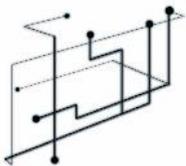
Pentaho - NOC Auto Detection



TOP SECRET STRAP 2

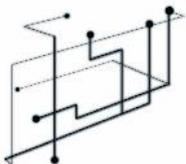
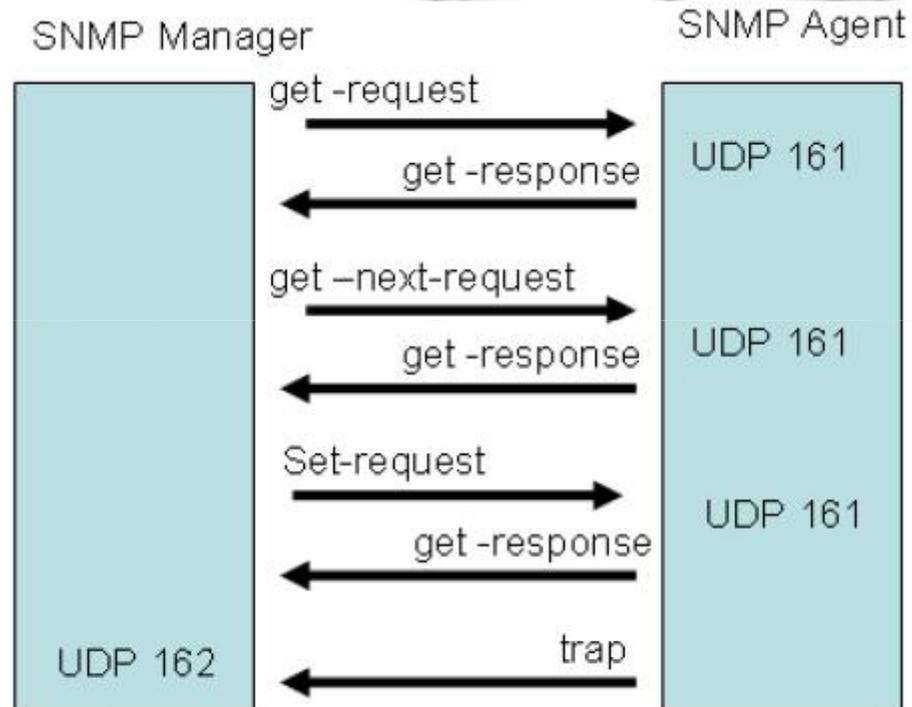
Phase 2: Intelligent use of Metadata

-
- 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



TOP SECRET STRAP 2

SNMP Protocol



TOP SECRET STRAP 2

SNMP Protocol in 5-Alive

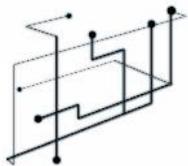
Options: ? Help | Filter | Export to CSV

Result	Time	Source	Destination	Protocol	Port	Country	Status		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
		[REDACTED]	[REDACTED]	-->	udp	[REDACTED]	161		
4	2011-05-13	09:59:37	[REDACTED]	-->	udp	[REDACTED]	161	US	Unknown
5	2011-05-13	09:59:36	[REDACTED]	-->	udp	[REDACTED]	161	US	Unknown
6	2011-05-12	07:22:32	[REDACTED]	-->	udp	[REDACTED]	161	LU	Unknown
7	2011-05-12	06:04:46	[REDACTED]	-->	udp	[REDACTED]	161	US	Unknown
8	2011-05-11	22:52:58	[REDACTED]	-->	udp	[REDACTED]	161	US	Unknown
9	2011-05-11	19:55:22	[REDACTED]	-->	udp	[REDACTED]	161	US	Unknown

TOP SECRET STRAP 2

Further drill down on activity for identified IP

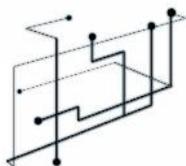
20		17	udp	DNS (Domain Name System)	63226	53	2011-05-12	07:30:00	2011-05-12	08:00:00
21		17	udp	Trivial File Transfer Protocol TFTP	52096	69	2011-05-13	10:00:00	2011-05-13	10:30:00
22		17	udp	Trivial File Transfer Protocol TFTP	58912	69	2011-05-13	10:00:00	2011-05-13	10:30:00
23		17	udp	Trivial File 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



TOP SECRET STRAP 2

From TCP Port 23 (Echo)

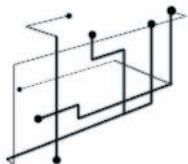
```
Untitled - Notepad
File Edit Format View Help

*****
* GRX kgli-ip1-r1.belbone.grx *
*****

*****
* UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS STRICTLY PROHIBITED. *
* You must have explicit permission to access or configure this device. *
* All activities performed on this device may be logged, and violations *
* of this policy may result in disciplinary action, and may be reported *
* to law enforcement... *
* There is no right to privacy on this device. *
* For more info mail to customer.care@belgacom-ics.com or tel +32 25475151 *
*****

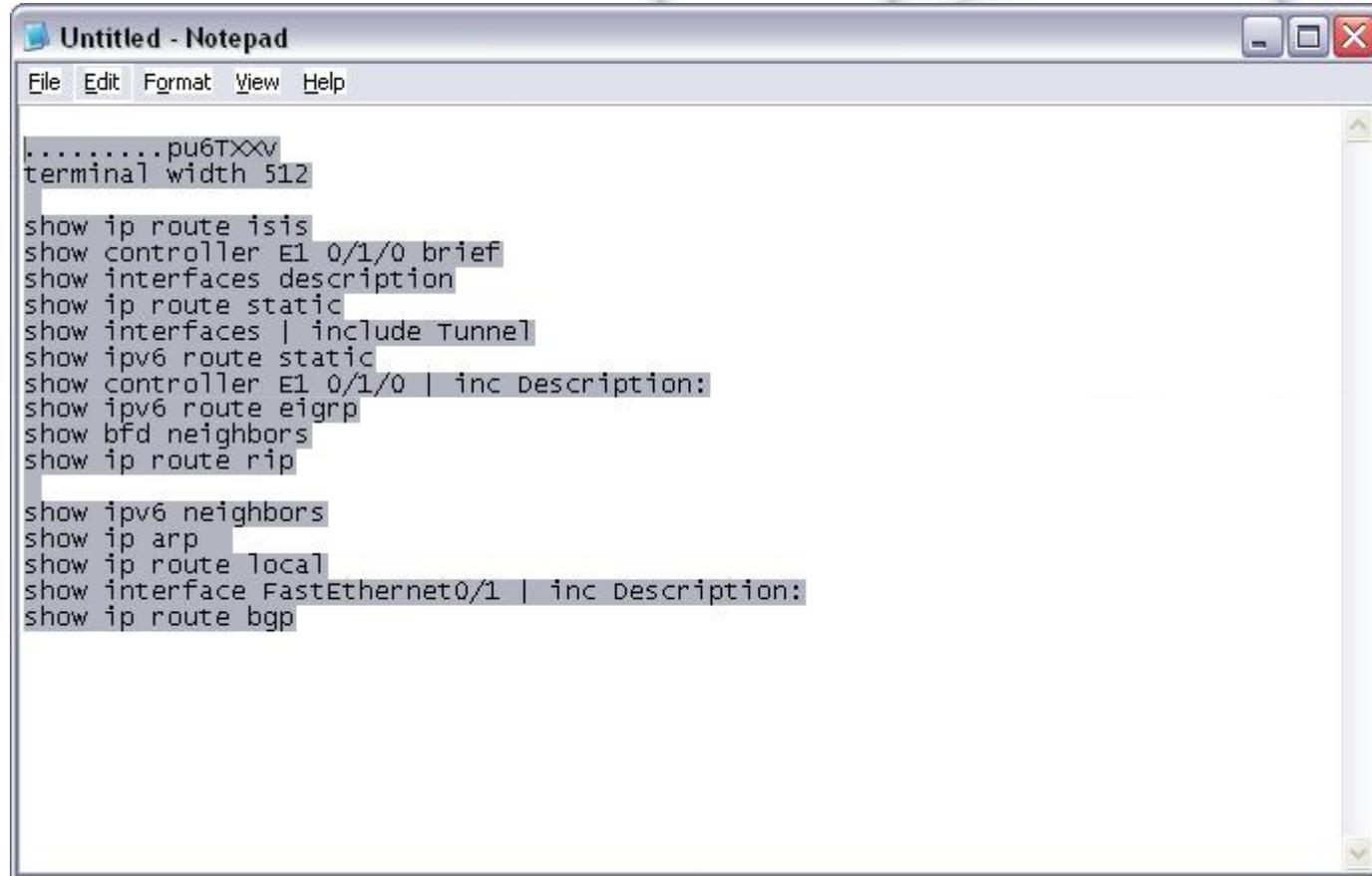
User Access Verification
Username: ..... ..!..!....."..'...rancid
Password:

kgli-ip1-r1>enable
Password:
kgli-ip1-r1#
kgli-ip1-r1#term length 0
kgli-ip1-r1#show version
```



TOP SECRET STRAP 2

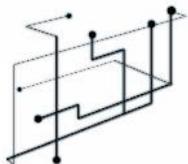
To TCP Port 23



```
.....pu6Txxv
terminal width 512

show ip route isis
show controller E1 0/1/0 brief
show interfaces description
show ip route static
show interfaces | include Tunnel
show ipv6 route static
show controller E1 0/1/0 | inc Description:
show ipv6 route eigrp
show bfd neighbors
show ip route rip

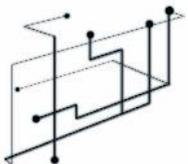
show ipv6 neighbors
show ip arp
show ip route local
show interface FastEthernet0/1 | inc Description:
show ip route bgp
```



TOP SECRET STRAP 2

Intelligent analysis of TELNET traffic

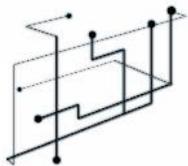
- The fact that login was successful for both examples means the following:
 - From TCP Port 23
 - To IP address is Network Management Terminal (in the NOC ?)
 - To TCP Port 23
 - From IP address is Network Management Terminal (in the NOC ?)



TOP SECRET STRAP 2

Phase 4: Bulk Port Scanning

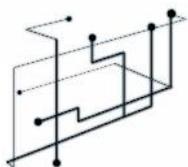
- We know the key services/servers running in the NOC
- Utilise HACIENDA, GCHQ's bulk port scanning capability to identify what IPs have these service ports open – additional logic to build up confidence required.



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.



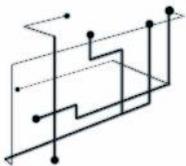
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ c [REDACTED]

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.



TOP SECRET STRAP 2

NOC IP range search in MUTANT BROTH

MUTANT BROTH

Identifier Search | IP Address Search | Password Search | **IP Prefix Search**

Legal Context

- This is a powerful technique that allows you to pull back presence events for an IP network.
- You **must** make sure that your HRA justification (Reason) clearly explains why you are querying on an IP network, as you are more likely to retrieve the communications of innocent individuals as well as targets.
- Your queries will be logged for audit.
- You should use Traceroute or DNS look up first so that only IP prefixes registered or associated with the target networks are queried.
- If you suspect that the IP prefix is dynamic, you must **either** combine this search with another filter eg an HHFP **or** limit the query length to 60 minutes.
- If after running the query, it is clear that the IP prefix is dynamic, you should not look at the results as they are unlikely to relate to your target.

Search for IP address prefixes

- Enter the set IP address prefixes.
- The IP address range must be specified as: < dotted decimal IP >/< prefix length >
- Example: 172.16.17.0/23
192.168.4.5
192.168.128.0/17
- Prefix lengths of less than 16 bits will be ignored.
- Absent lengths are assumed to be 32 bits.
- Optionally enter the HHFP or the time period start and search length in minutes.

IP Ranges:

HHFP:

Time period start:

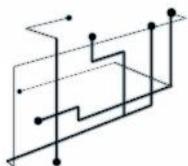
Search length (minutes):

MIRANDA:

JIC:

Purpose:

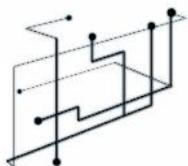
Reason:



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		(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

This information is exempt from disclosure under [redacted] legislation. Refer disclosure requests to GCHC [redacted] exemption under other UK information

TOP SECRET STRAP 2

Real-time picture of QI

NRTA Dashboard - Mozilla Firefox

up to TOP SECRET STRAP 2 UK EYES ONLY

NRTA Dashboard for INOC Alerts for OPSOCIALIST

Target	TDI Type	Selector	IP addresses	Age	From	To	OS
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.143.99	0 minutes ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63
[REDACTED]	LinkedIn-Member	[REDACTED]	Route: 91.181.245.18 Src: 91.181.245.18; Dest: 216.52.242.88	14.28 hours ago	[REDACTED]	[REDACTED]	Firefox 3.6.13
[REDACTED]	LinkedIn-Member	[REDACTED]	Route: 93.184.208.58 Src: 93.184.208.58; Dest: 216.52.242.82	18.17 hours ago	[REDACTED]	[REDACTED]	Safari 4.0
[REDACTED]	LinkedIn-Member	[REDACTED]	Route: 178.144.30.204 Src: 178.144.30.204; Dest: 216.52.242.88	20.11 hours ago	[REDACTED]	[REDACTED]	Safari 4.0
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 10.252.243.17 Src: 10.252.243.17; Dest: 10.225.65.192	22.56 hours ago	[REDACTED]	[REDACTED]	
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.143.104	23.48 hours ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 10.252.243.5 Src: 10.252.243.5; Dest: 10.225.31.68	24.24 hours ago	[REDACTED]	[REDACTED]	
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 10.252.243.11 Src: 10.252.243.11; Dest: 10.225.31.199	24.58 hours ago	[REDACTED]	[REDACTED]	
[REDACTED]	Google-PREFID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.143.104	25.03 hours ago	[REDACTED]	[REDACTED]	Firefox 3.6.13
[REDACTED]	LinkedIn-Member	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 216.52.242.88	26.14 hours ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63

GeoIPinfo reports IP address 213.181.44.4 as MECHELEN (low confidence), BE (high confidence).
No results returned.

Date	Time (UTC)	Source	Destination	Type	Description
11/02/11	14:56:23	213.181.44.4:80752459	195.125.115.181	HTTPFormPOST	POST to widget.samsungmobile.com/NPS/UpdateMagerService/Service1.aspx/GetMatchHotfy
11/02/11	14:56:14	213.181.44.4:9b0M290	46.137.114.64	HTTP	GET rainbow.mythings.com [REDACTED]
11/02/11	14:56:14	213.181.44.4:9b0M290	79.125.107.244	HTTP	GET pixel.rubiconproject.com/tab.php?y=566011
11/02/11	14:56:03	213.181.44.4:80752459	195.125.115.181	HTTPFormPOST	POST to widget.samsungmobile.com/NPS/UpdateMagerService/Service1.aspx/GetMatchHotfy
11/02/11	14:55:59	213.181.44.4:9b0M290	46.137.114.64	HTTP	GET rainbow.mythings.com [REDACTED]
11/02/11	14:55:56	213.181.44.4:441e94ee	46.137.126.199	HTTP	GET synchrobox.adswizz.com [REDACTED]
11/02/11	14:55:46	213.181.44.4:441e94ee	46.137.126.199	HTTP	GET synchrobox.adswizz.com [REDACTED]
11/02/11	14:55:42	213.181.44.4:80752459	195.125.115.181	HTTPFormPOST	POST to widget.samsungmobile.com/NPS/UpdateMagerService/Service1.aspx/GetMatchHotfy

Expand all Collapse all Export CSV Export raw

3/3 66 Row(s)

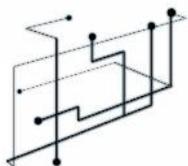
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED] (for UK information legislation).



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

Questions ?



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or [REDACTED]