

AND THEY SAID TO THE TITANS: « WATCH OUT OLYMPIANS IN THE HOUSE! »

**CSEC – Advanced Network Tradecraft
SD Conference June 2012**

Overall Classification: TOP SECRET//SI

OLYMPIA & THE CASE STUDY



CSEC's Network Knowledge Engine

- Various data sources
- Chained enrichments
- Automated analysis

Brazilian Ministry of Mines and Energy (MME)

- New target to develop
- Limited access/target knowledge

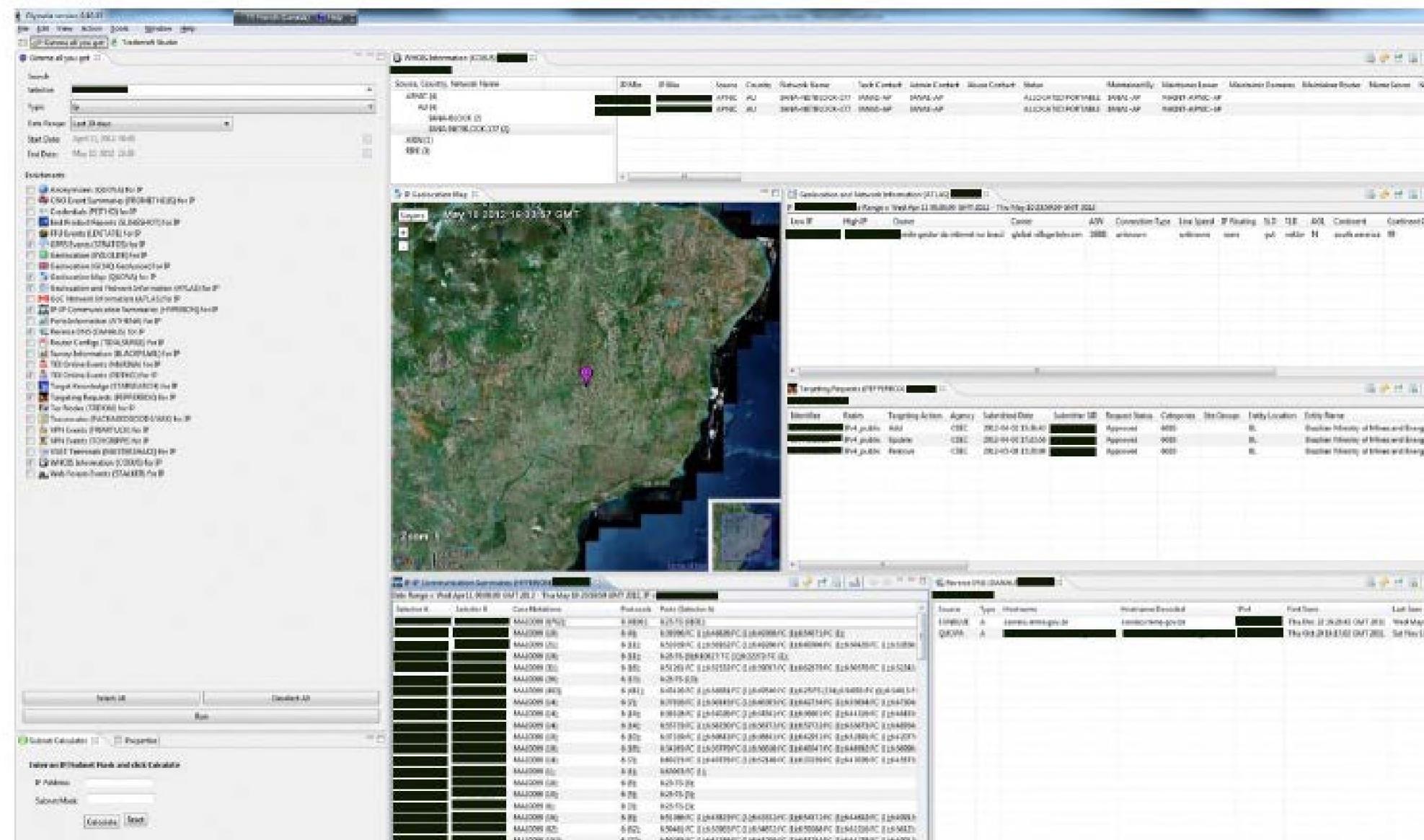


QUESTIONS

- How can I use the information available in SIGINT data sources to learn about the target?
- What can I find that would help me inform access development efforts?
- Can I automate the analytical process and/or re-use analytics designed for other purposes?



OLYMPIA AT A GLANCE



1

OLYMPIA AT A GLANCE

OLYMPIA version 0.0.25

File Edit View Action Tools Options Help

☰ [Search] Information [CSV] [Print] [Help]

☰ [Search] Information [CSV] [Print] [Help]

Source, Country, Network Name:

IP Address	IP Mask	Source	Country	Network Name	Tech Contact	Admin Contact	Maint Contact	Status	Maintained By	Maintenance Logon	Maintenance Domain	Maintenance Router	Name Server	None
192.168.1.1	255.255.255.0	APNIC	US	192.168.1.1/24-177	192.168.1.1	192.168.1.1	192.168.1.1	ALLOCATED PORTABLE	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
192.168.1.2	255.255.255.0	APNIC	US	192.168.1.2/24-177	192.168.1.2	192.168.1.2	192.168.1.2	ALLOCATED PORTABLE	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2
192.168.1.3	255.255.255.0	APNIC	US	192.168.1.3/24-177	192.168.1.3	192.168.1.3	192.168.1.3	ALLOCATED PORTABLE	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3

Search:

Type: IP

Date Range: Last 30 days

Start Date: April 10, 2012 00:00

End Date: May 10, 2012 23:59

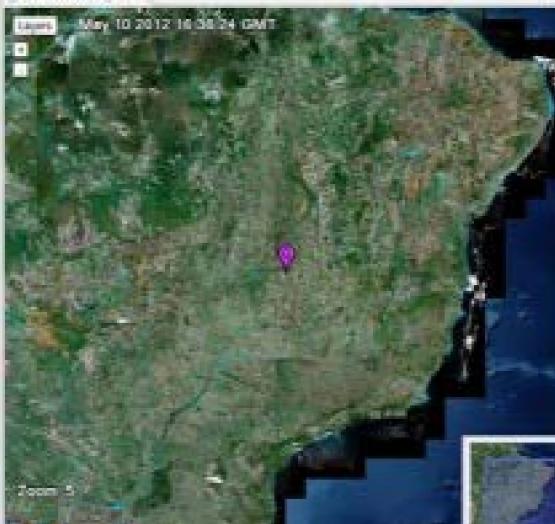
Search Results:

- Anonymizes (QUOVA) for IP
- CNO Event Summaries (PROMETHEUS) for IP
- Credentials (PBTHO) for IP
- End Product Reports (SLINGSHOT) for IP
- FFI Events (MARINA) for IP
- GPRS Events (STRATOS) for IP
- Geolocation (EVOLVE) for IP
- Geolocation (GCHQ Geofusion) for IP
- Geolocation Map (QUOVA) for IP
- Geolocation and Network Information (ATLAS) for IP
- GoC Network Information (ATLAS)
- IP-IP Communication Summaries (HYPERION)
- Ports Information (ATHENA)
- Reverse DNS (DANAU)
- Router Config (TIDAL-SURGE)
- Survey Information (BLACKPEARL)
- TDI Online Events (MARINA)
- TDI Online Events (PBTHO)
- Target Knowledge (STARSEARCH)
- Targeting Requests (PEPPERBOX)
- Tor Nodes (TRITON)
- Tracesoutes (PACKAGEDGOODS/ARK)
- VPN Detailed Events (TOYGRIPPE)
- VPN Events (FBARTUCK)
- VPN Events (TOYGRIPPE)
- VSAT Terminals (MASTERSHARE)
- WHOIS Information (COEUS)
- Web Forum Events (STALKER)

Geolocation and Network Information (ATLAS)

Date Range: Last Day (11-May-2012 00:00:00 GMT - 12-May-2012 23:59:59 GMT)

Loc IP: High IP: Source: Center: ASN: Connection Type: Line Speed: IP Routing: S.D.: T.S.: ATs: Countries: Continents: IP



Anonymizes (QUOVA)

CNO Event Summaries (PROMETHEUS)

Credentials (PBTHO)

End Product Reports (SLINGSHOT)

FFI Events (MARINA)

GPRS Events (STRATOS)

Geolocation (EVOLVE)

Geolocation (GCHQ Geofusion)

Geolocation Map (QUOVA)

Geolocation and Network Information (ATLAS)

GoC Network Information (ATLAS)

IP-IP Communication Summaries (HYPERION)

Ports Information (ATHENA)

Reverse DNS (DANAU)

Router Config (TIDAL-SURGE)

Survey Information (BLACKPEARL)

TDI Online Events (MARINA)

TDI Online Events (PBTHO)

Target Knowledge (STARSEARCH)

Targeting Requests (PEPPERBOX)

Tor Nodes (TRITON)

Tracesoutes (PACKAGEDGOODS/ARK)

VPN Detailed Events (TOYGRIPPE)

VPN Events (FBARTUCK)

VPN Events (TOYGRIPPE)

VSAT Terminals (MASTERSHARE)

WHOIS Information (COEUS)

Web Forum Events (STALKER)

Request ID: Request Status: Category: Site Group: Entry Location: Entry Name:

city	Approved	000	00	Broadband Ministry of Mines and Energy
city	Approved	000	00	Broadband Ministry of Mines and Energy
city	Approved	000	00	Broadband Ministry of Mines and Energy

Monitoring Created: IP: Fire Seen: Last Seen:

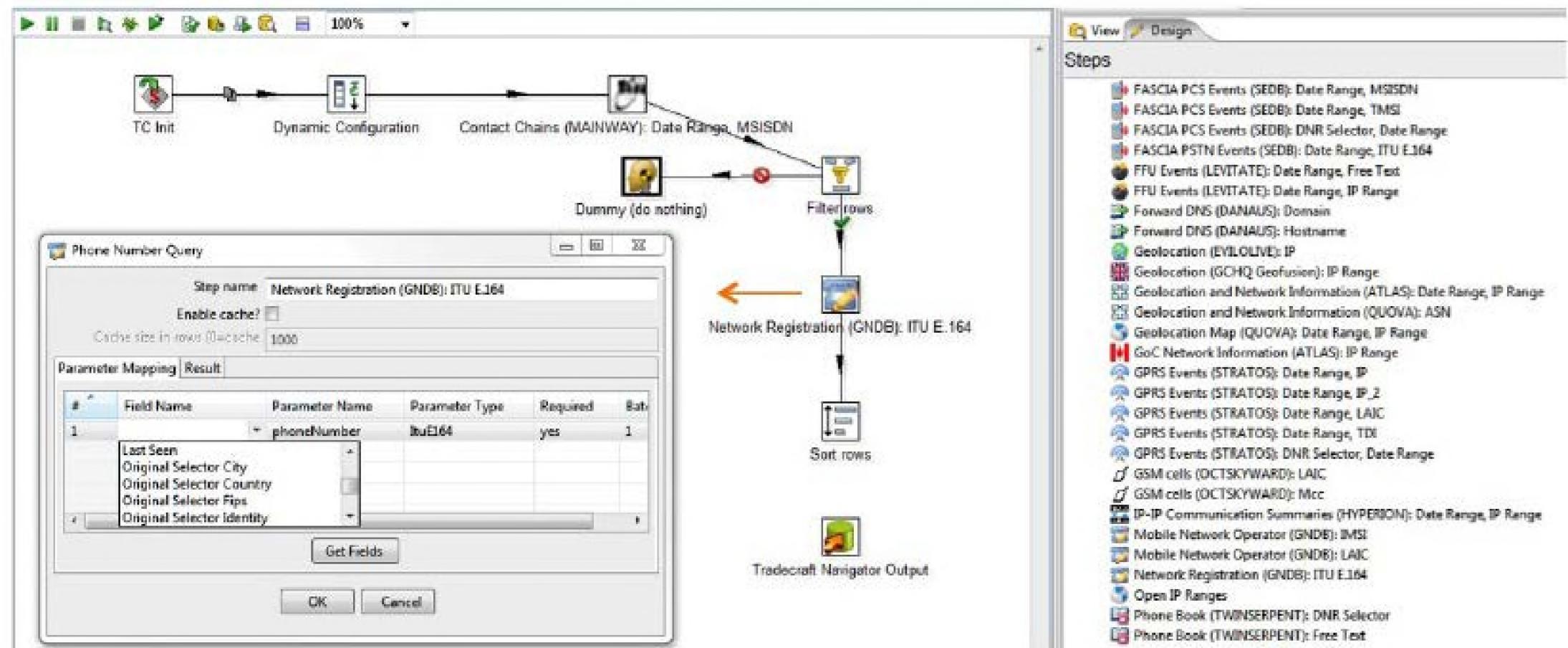
Fire Seen: Last Seen:

Hosts with IP: IP: Fire Seen: Last Seen:

Fire Seen: Last Seen:



OLYMPIA - AUTOMATION



Numerous enrichment and data manipulation nodes
Drag and drop each node
Create links between nodes
Hit the *Play* button

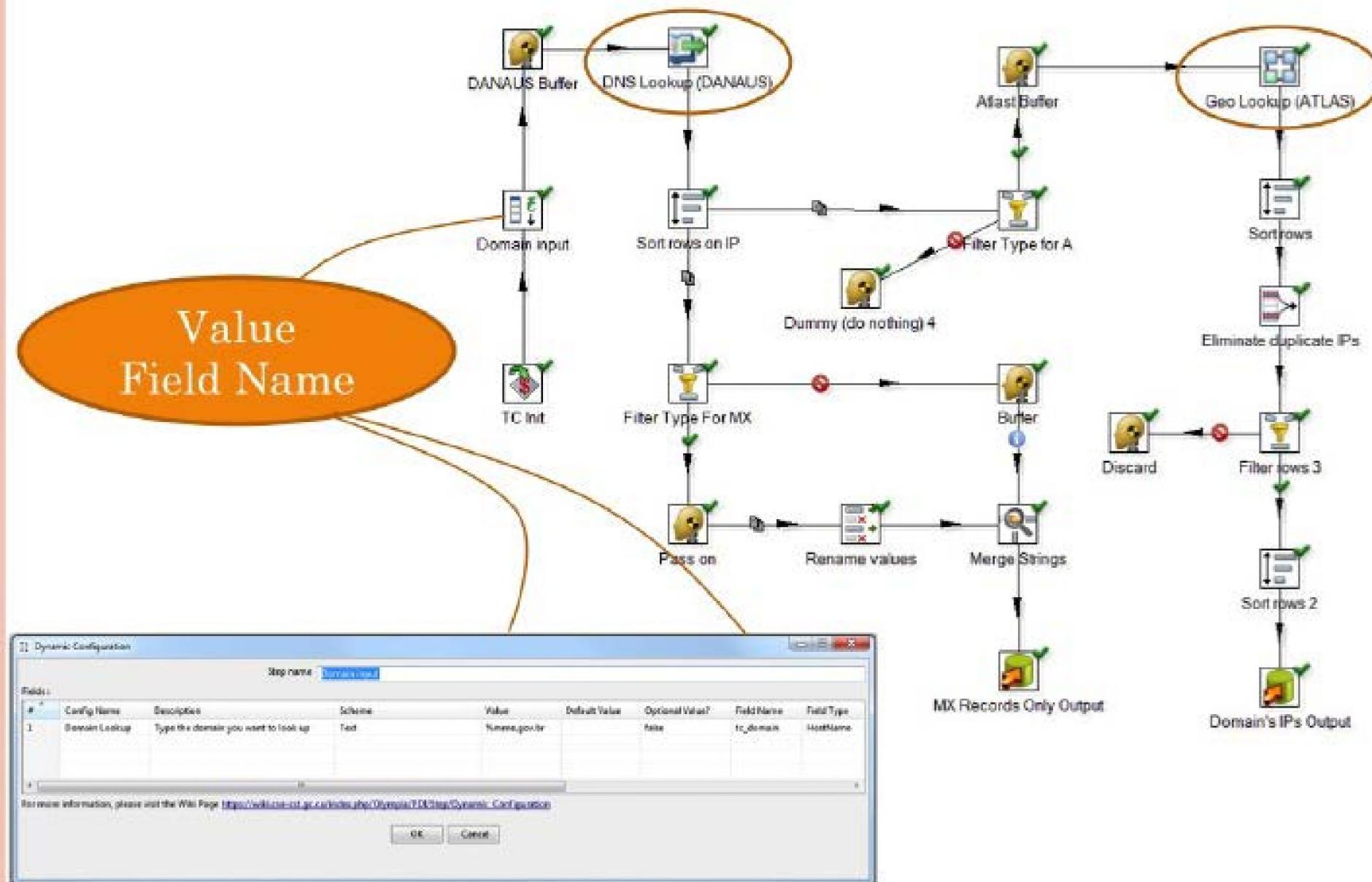
ANALYSIS – CASE STUDY

What we know about the target:

- Domain: @mme.gov.br
- 9 DNR selectors
- Very little collection



ANALYSIS – DETERMINE TARGET'S IPS AND ISPs



ANALYSIS – DETERMINE TARGET'S IPS AND ISPS

Mail Servers Output

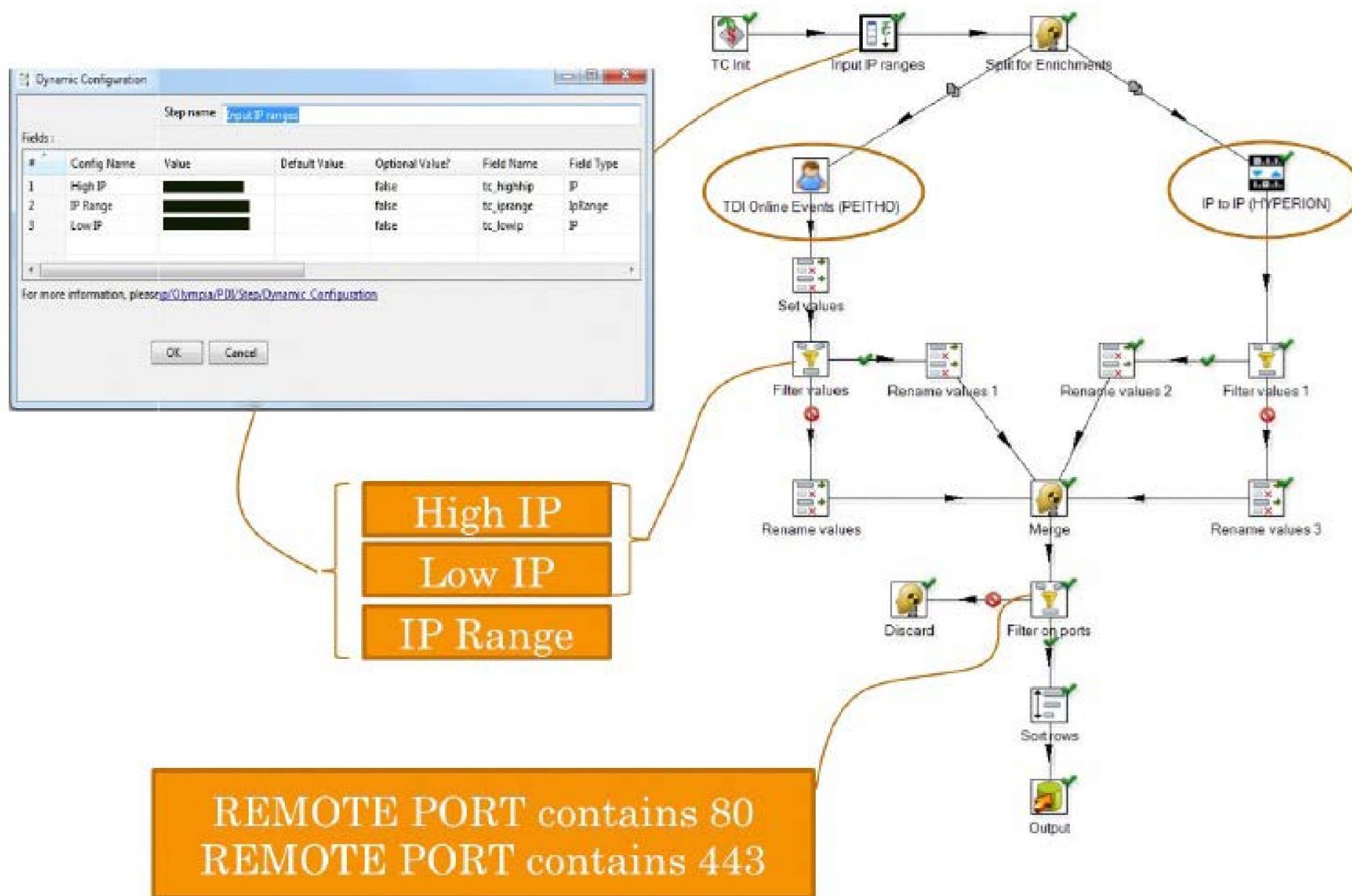
Response_MX	Hostname	IPv4	Source	First Seen	Last Seen
correo.mme.gov.br	correo.mme.gov.br	[REDACTED]	EONBLUE	Wed Jun 17 06:04:23 GMT 2009	Mon Feb 15 12:40:53 GMT 2010
correo2.mme.gov.br	correo2.mme.gov.br	[REDACTED]	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011

Domain's IPs Output

Type	Hostname	IPv4	IP Range	Country	ASN	Owner	Carrier	Source	First Seen	Last Seen
A	ns1.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16881	comite gestor da internet no brasil	global village idcom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 22:49:36 GMT 2011	Sat May 05 10:05:59 GMT 2012
A	ns2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Tue May 08 17:28:22 GMT 2012
A	sn01.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16881	comite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Wed Apr 25 04:55:02 GMT 2012
A	correo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16881	comite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 16:26:42 GMT 2011	Wed May 02 21:11:17 GMT 2012
A	acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	ns1.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	correo2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Feb 11 13:15:47 GMT 2010	Mon Dec 19 19:40:43 GMT 2011
A	nc2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Sep 15 23:11:09 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	sn01.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Thu Mar 03 19:37:08 GMT 2011	Tue Dec 20 15:49:18 GMT 2011
A	prodeum.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	sn01.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Wed Feb 10 12:31:14 GMT 2010	Tue Sep 07 09:24:13 GMT 2010
A	correo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	EONBLUE	Fri Feb 12 20:14:25 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	correo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16954	comite gestor da internet no brasil	sepro	QUOVA	Thu Feb 19 20:07:34 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	correo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16954	comite gestor da internet no brasil	sepro	QUOVA	Fri Mar 27 14:03:47 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	urano.mme.gov.br	[REDACTED]	[REDACTED]	brazil	16954	comite gestor da internet no brasil	sepro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	terramme.gov.br	[REDACTED]	[REDACTED]	brazil	16954	comite gestor da internet no brasil	sepro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:23:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:43 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	webpac.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:23:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	prodeum.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:43 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	urano.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	terramme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon Apr 20 11:24:46 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	correo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	comite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:43 GMT 2010	Sat Nov 19 01:52:58 GMT 2011

Hostname
IPv4
Country
ASN
Owner
Carrier

ANALYSIS – DISCOVER TARGET'S PROXY



ANALYSIS – DISCOVER TARGET'S PROXY

Entity IP :

[REDACTED]

Remote IP : various

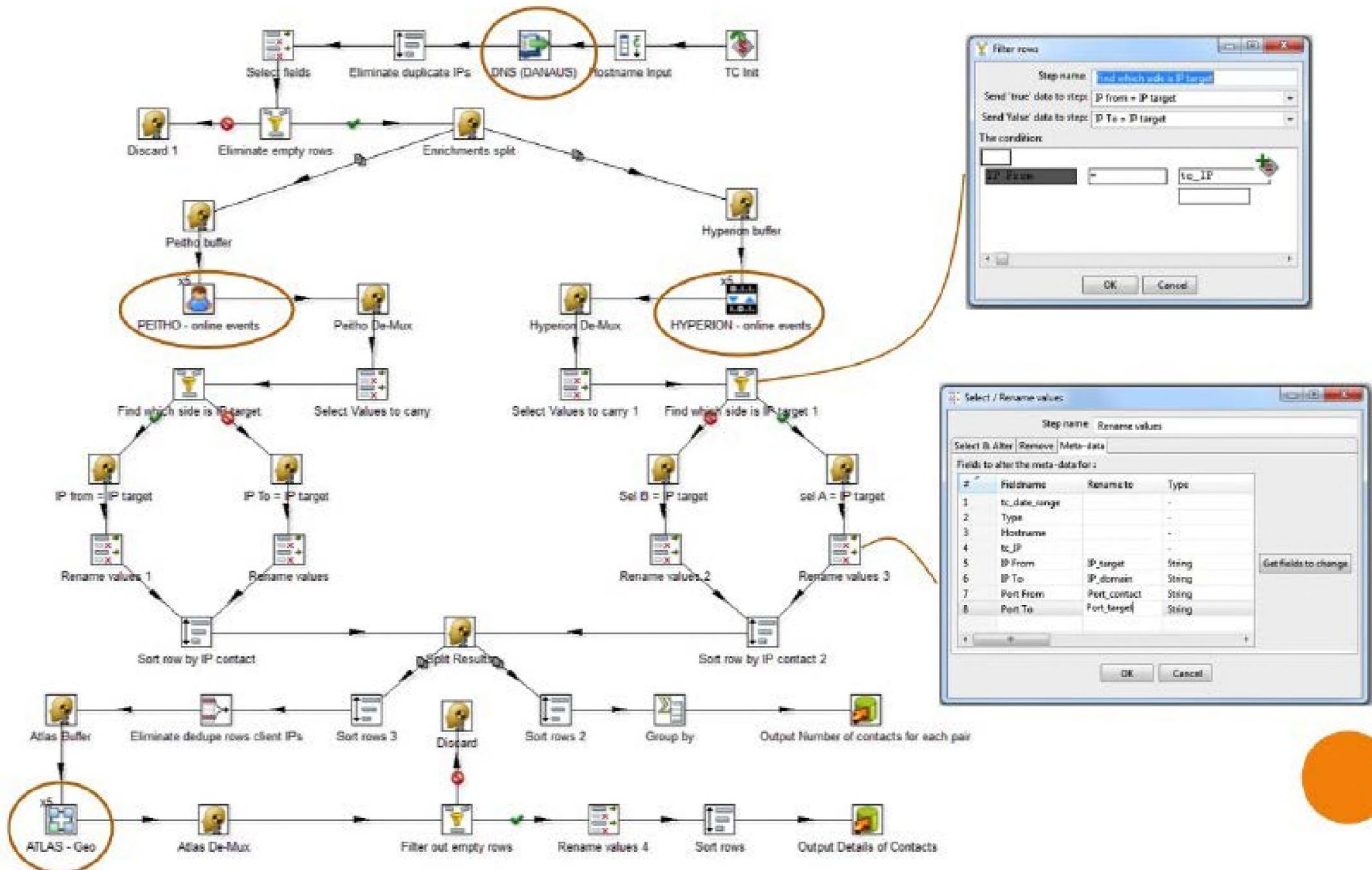
Remote Port : 443

Entity Port: various

Target Proxy Output

entity_ip	remote_ip	remote_port	entity_port
[REDACTED]	[REDACTED]	6:443:TS (1);	6:47367:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:27973:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:48329:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (2);	6:47950:FC (1);6:4834
[REDACTED]	[REDACTED]	6:443:TS (2);	6:54695:FC (1);6:4358
[REDACTED]	[REDACTED]	6:443:TS (4);	6:31670:FC (1);6:3432
[REDACTED]	[REDACTED]	6:443:TS (5);	6:1263:FC (1);6:4115
[REDACTED]	[REDACTED]	6:443:FS (12);	6:48927:TC (1);6:4893
[REDACTED]	[REDACTED]	6:443:TS (179);6:80:16:26704:FC (1);6:2670	
[REDACTED]	[REDACTED]	6:443:TS (1);	6:11217:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (165);	6:12946:FC (1);6:1523
[REDACTED]	[REDACTED]	6:443:TS (1);	6:60657:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (1);	6:45811:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (14);6:80:TS 6:19170:FC (2);6:5364	

ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH



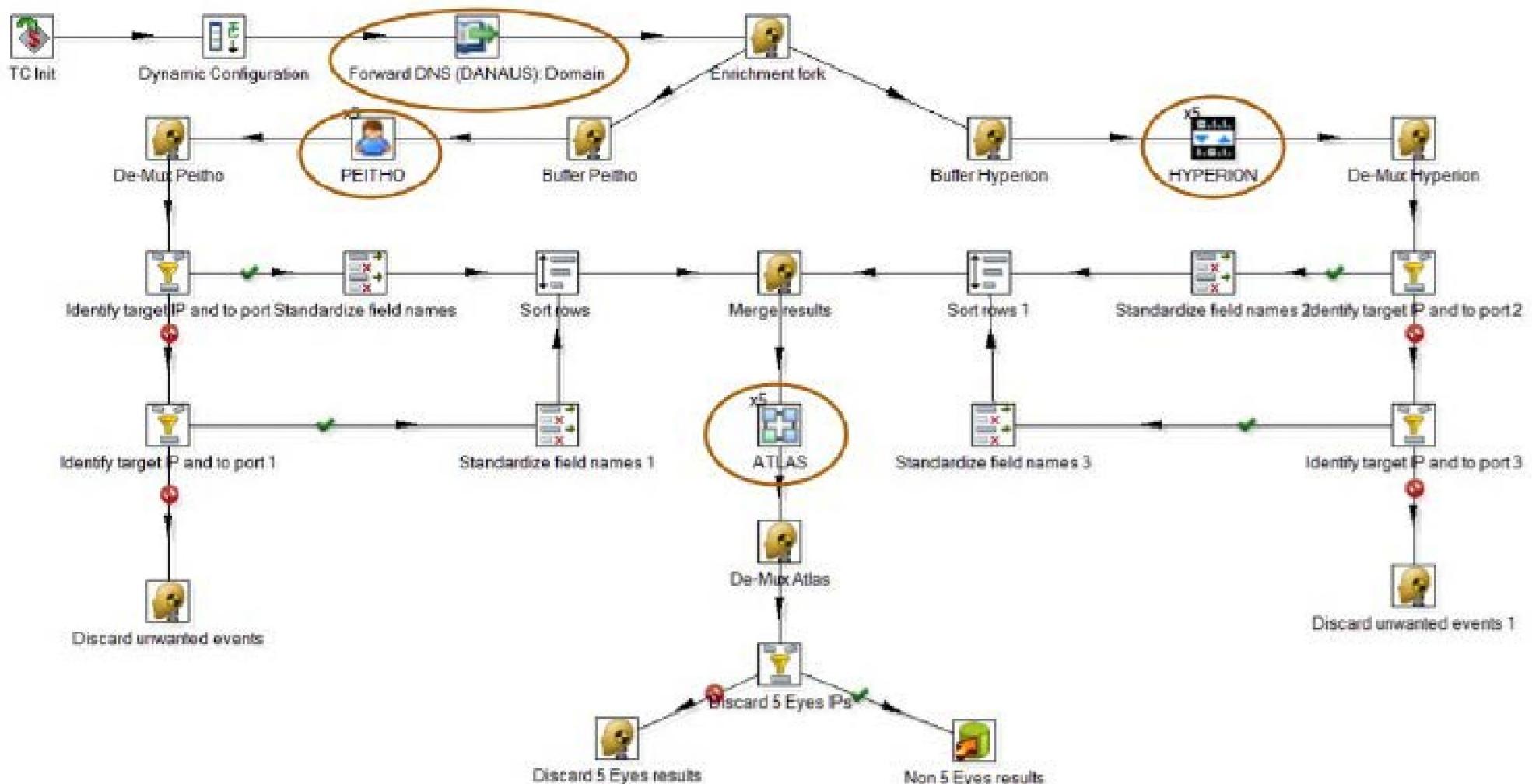
ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

Hostname domain	IP domain	IP in contact with domain	Port used by IP domain	Port used by IP contact	Owner of IP contact	Carrier of IP contact	ASN of IP contact	Country of IP contact	IP range for IP contact
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:61391:FC (1);	tse.i.net.noc.ip.infrastructure	british telecommunications plc	3400	eritrea	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:69181:FC (1);	tse.i.net.noc.ip.infrastructure	british telecommunications plc	3400	eritrea	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (2);6:25:FS (1);	6:54251:FC (2);	tata communications	tata communications	6453	canada	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:28151:FC (1);	jdc	jordan telecommunications com	3697	jordan	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:2990:FC (1);	resign to idc-dbw-idc customers for info public company limited	9891	thailand	[REDACTED]	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:50072:TC (1);	internal network	international data exchange llc	12924	jordan	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:51934:FC (1);	pers online	personline	16322	iran	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:2295:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:1799:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:50329:FC (1);	dsl home subscribers	saudinet	25019	saudi arabia	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (1);	6:22423:FC (1);	saudinet saudi telecom company saudinet	25019	saudi arabia	[REDACTED]	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:54396:TC	6:25:75 (128);	iweb dedicated hd	iweb technologies inc.	32613	canada	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:33907:TC	6:25:75 (22);	iweb dedicated hd	iweb technologies inc.	32613	canada	[REDACTED]
correio.mme.gov.br	[REDACTED]	[REDACTED]	6:25:73 (4);	6:57773:FC	middle east internet company llc cyberian yadh		34397	saudi arabia	[REDACTED]
www.mme.gov.br	[REDACTED]	[REDACTED]	6:80:73 (1);	6:54791:TC (1);	adsl service	sahara net	41576	saudi arabia	[REDACTED]

Hostname starting domain
 IP starting domain
 IP in contact with starting domain
 Port used by starting domain
 Port used by IP contact

Owner of IP contact
 Carrier of IP contact
 ASN of IP contact
 Country of IP contact
 IP range for IP contact

ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET



ANALYSIS – IDENTIFY POTENTIAL MAN ON THE SIDE OPERATION AGAINST MY TARGET

Results

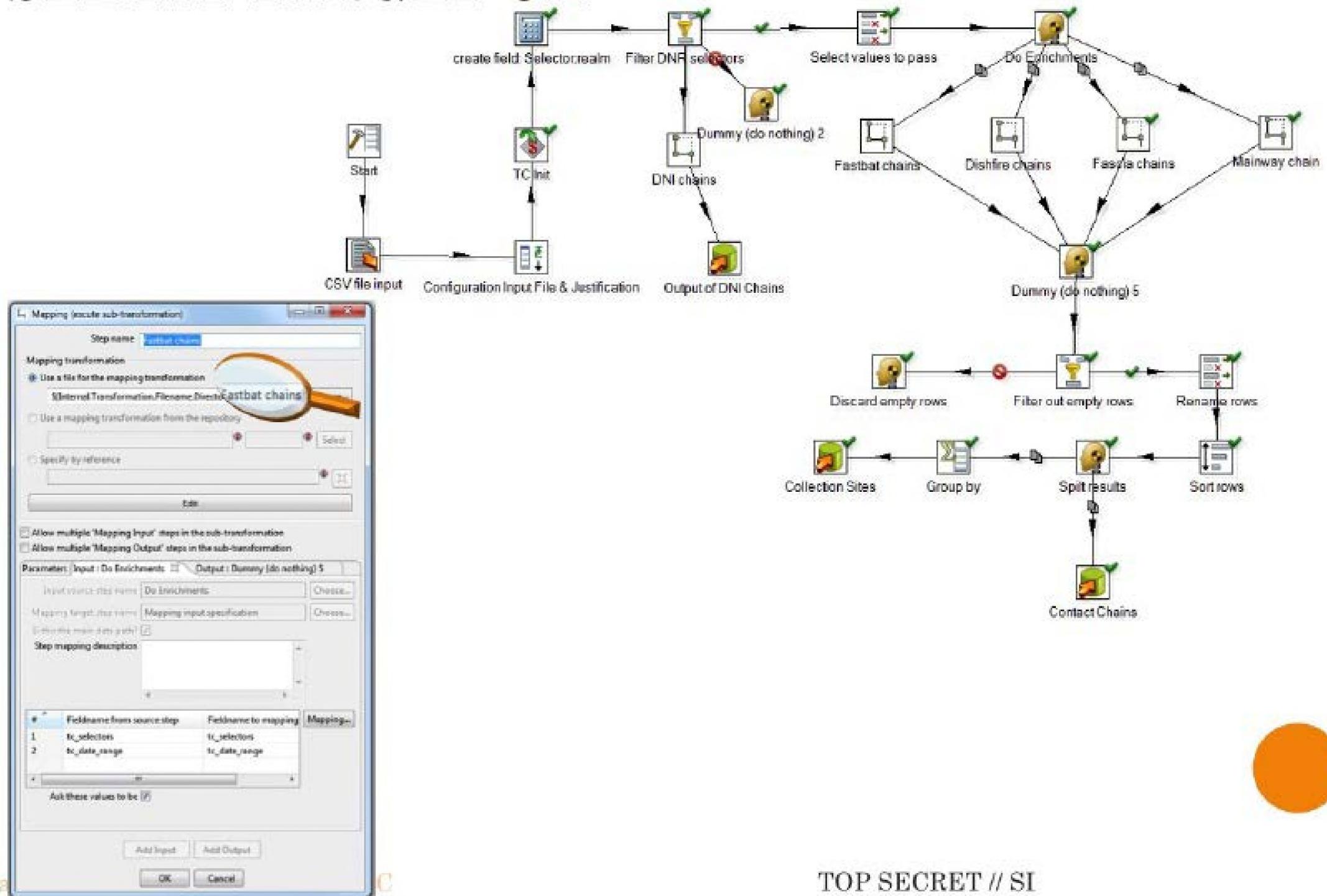
target_hostname	target	contact	target_port	contact_port	Case Notations	Country	Digraph
[acessovpn.mme.gov.br]	[REDACTED]	[REDACTED]	6:41278:TC (1):	6:80:FS (1):	MA10099 (1):	brazil	br
acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	6:30141:TC (1):	6:80:FS (1):	MA10099 (1):	brazil	br

ASN contact	Country contact	# IPs contact
18891	brazil	26
7738	brazil	11
26599	brazil	6
19182	brazil	3
10429	brazil	2
27717	brazil	2
53006	brazil	2
14080	colombia	1
16735	brazil	1
32613	brazil	1
52972	brazil	1
8151	mexico	1

ASN contact	Country contact	# IPs contact
18891	brazil	15
26599	brazil	9
10429	brazil	7
16735	brazil	5
18479	brazil	3
45774	india	3
7738	brazil	3
19182	brazil	2
27699	brazil	2
13878	brazil	1
14080	colombia	1
16509	brazil	1
17379	brazil	1
28311	brazil	1
28670	brazil	1
32613	brazil	1
4808	china	1
53018	brazil	1
53070	brazil	1
9829	india	1

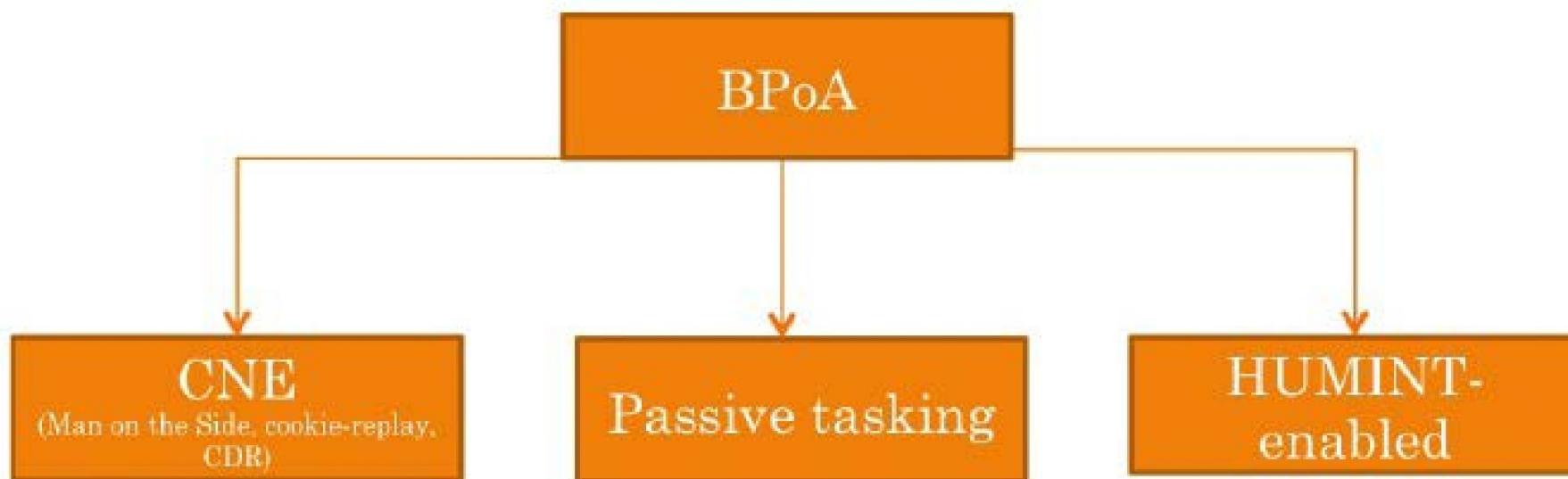
Reverse DNS (IANA) for IP 129.121.12.12				
P = 129.121.12.12	Source	Type	Hostname	Hostname Decoded
	EONBLUE	A	www.entre.net.br	www.entre.net.br
	EONBLUE	A	sinergia.com.br	sinergia.com.br
	EONBLUE	A	transformadivisao.com.br	transformadivisao.com.br
	EONBLUE	A	geoferatu.br	geoferatu.br
	EONBLUE	A	multibras.com.br	multibras.com.br
	EONBLUE	A	tricampus.edu.br	tricampus.edu.br
	EONBLUE	A	abdcv.com.br	abdcv.com.br
	EONBLUE	A	hellenweb.org.br	hellenweb.org.br
	EONBLUE	A	afabip.com.br	afabip.com.br
	EONBLUE	A	advcc.com.br	advcc.com.br
	EONBLUE	A	metajato.com.br	metajato.com.br
	EONBLUE	A	guridoro.com.br	guridoro.com.br
	EONBLUE	A	atq.com.br	atq.com.br
	EONBLUE	A	batopress.com.br	Batopress.com.br
	EONBLUE	A	mtvvisagens.com.br	mtvvisagens.com.br
	EONBLUE	A	stephanot.com.br	stephanot.com.br
	EONBLUE	A	2houzinovels.com.br	2houzinovels.com.br
	EONBLUE	A	thati.com.br	thati.com.br
	EONBLUE	A	gafis.com.br	gafis.com.br
	EONBLUE	A	edpch.com.br	edpch.com.br
	EONBLUE	A	institutodepv.org	institutodepv.org

ANALYSIS – DISCOVER CONTACTS OF MY TARGET AND COLLECTION SITES I SEE MY TARGET ON



SUMMARY

Based on the information collected, I am better positioned to analyse my target's telecoms environment.



MOVING FORWARD

- I have identified MX servers which have been targeted to passive collection by the Intel analysts, who are assessing the value, provenance, etc. of the traffic generated by the mail servers.
- I am working with TAO to further examine the possibility for a Man on the Side operation.
- Based on the network information gathered, the NAC has started a BPoA analysis on the MME.

