



**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



OLYMPIA

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 reuse analytics designed for other purposes?



OLYMPIA AT A GLANCE

The screenshot displays the Olympia system interface with several active windows:

- WFOC Information (WFOC):** A table listing network information with columns for Source, Location, Network Name, ZONE, IP Size, Source, Country, Network Name, Tech Contact, Service Contact, Status, Maintenance, Maintenance Issues, Maintenance Comments, Maintenance Router, Maintenance Status, and Web.
- Geographic Map:** A satellite map of the Pacific Northwest region with a purple location marker.
- Geographic and Network Information (GFI):** A table with columns for Low IP, High IP, Name, Color, ASN, Connection Type, Line Speed, IP Routing, SD, QoS, QoS, Contact, and ContactID.
- Targeting/Requests (TRP):** A table with columns for Identifier, Status, Targeting Action, Agency, Submitted Date, Submitted By, Request Status, Category, Sub-Group, Entry Location, and Entry Name.
- Networks (N):** A table with columns for Source, Type, Hostname, Hostname Encoded, IPid, First Seen, and Last Seen.
- Networks Summary (NS):** A table with columns for Identifier, Location, Capabilities, Network, and Data (Source ID).
- Search:** A sidebar on the left containing search filters for Name, Type, Line Speed, Start Date, and End Date, along with a list of search results.
- Global Calculator:** A small utility window at the bottom left with input fields for IP Address and Subnet Mask, and buttons for Calculate and Reset.



OLYMPIA AT A GLANCE

The screenshot displays the OLYMPIA software interface with several active panels:

- Search Panel (Top Left):** Includes a search bar, a dropdown menu for 'Type', and date range filters for 'Start Date' and 'End Date'.
- IP Information Panel (Top Center):** A table listing IP addresses, their source countries (e.g., APNIC), and associated network names.
- IP Geolocation Map (Center):** A satellite map of Africa with a purple location pin. The map title is 'IP Geolocation Map' and the date is 'May 10 2012 10:38:24 GMT'.
- IP-IP Communication Summaries Panel (Bottom Center):** A table showing communication data between IP addresses.
- Navigation Panel (Right Side):** A vertical list of application icons and names, including:
 - Anonymizers (QUOVA)
 - CNO Event Summaries (PROMETHEUS)
 - Credentials (PEITHO)
 - End Product Reports (SLINGSHOT)
 - FFU Events (LEVITATE)
 - GPRS Events (STRATOS)
 - Geolocation (EVOLVE)
 - Geolocation (GCHQ Geolusion)
 - Geolocation Map (QUOVA)
 - Geolocation and Network Information (ATLAS)
 - GoC Network Information (ATLAS)
 - IP-IP Communication Summaries (HYPERION)
 - Ports Information (ATHENA)
 - Reverse DNS (DANAUS)
 - Router Configs (TIDALSURGE)
 - Survey Information (BLACKPEARL)
 - TDI Online Events (MARINA)
 - TDI Online Events (PEITHO)
 - Target Knowledge (STARSEARCH)
 - Targeting Requests (PEPPERBOX)
 - Tor Nodes (TRITON)
 - Traceroutes (PACKAGEDGOODS/ARK)
 - VPN Detailed Events (TOYGRIPPE)
 - VPN Events (FRSARTUCK)
 - VPN Events (TOYGRIPPE)
 - VSAT Terminals (MASTERSHAKE)
 - WHOIS Information (COEUS)
 - Web Forum Events (STALKER)
- Data Tables (Right Side):** Two tables displaying event and communication data with columns for 'Event ID', 'Request Status', 'Categories', 'Site Groups', 'Entity Location', and 'Entity Name'.



OLYMPIA - AUTOMATION

The screenshot displays the OLYMPIA automation interface. The main workspace shows a workflow diagram with the following steps: TC Init, Dynamic Configuration, Contact Chains (MAINWAY): Date Range, MSISDN, Dummy (do nothing), Filter rows, Network Registration (GNDB): ITU E.164, Sort rows, and Tradecraft Navigator Output. A 'Phone Number Query' dialog box is open, showing a table for parameter mapping.

#	Field Name	Parameter Name	Parameter Type	Required	Bat.
1	phoneNumber	ITU E.164		yes	1

The dialog box also includes a 'Get Fields' button and 'OK'/'Cancel' buttons. A 'Steps' list on the right side of the interface contains various enrichment and data manipulation nodes, such as 'FASCIA PCS Events (SEDB): Date Range, MSISDN', 'Geolocation (EVLOLIVE): IP', and 'Network Registration (GNDB): ITU E.164'. An orange arrow points from the 'Network Registration (GNDB): ITU E.164' node in the workflow to the corresponding entry in the 'Steps' list.

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

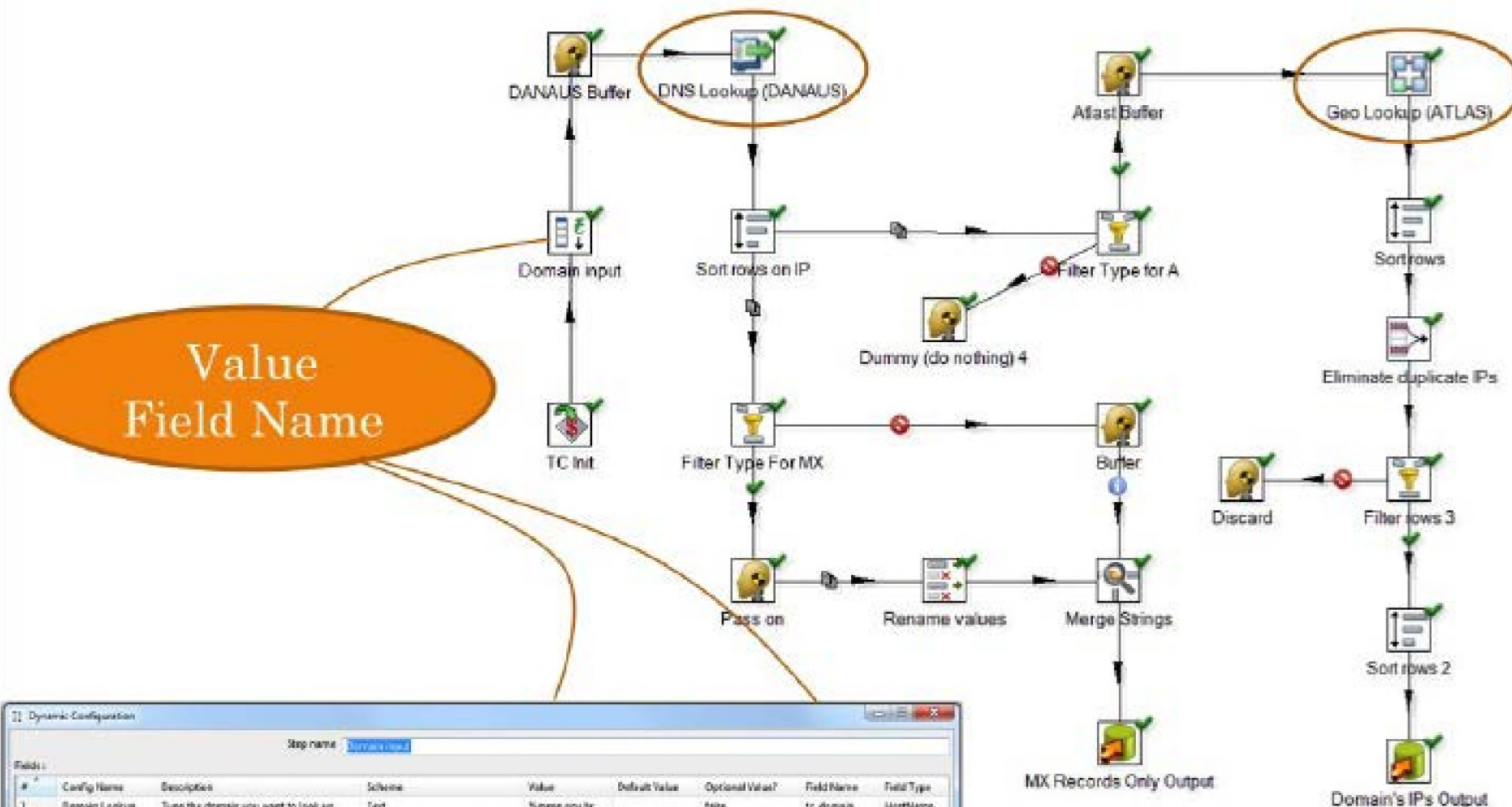
ANALYSIS – CASE STUDY

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
comeio.mme.gov.br	comeio.mme.gov.br	[REDACTED]	EONBLUE	Wed Jun 17 06:04:23 GMT 2009	Mon Feb 15 12:40:53 GMT 2010
comeio2.mme.gov.br	comeio2.mme.gov.br	[REDACTED]	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011

Hostname
 IPv4
 Country
 ASN
 Owner
 Carrier

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	18881	cemite 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	www.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	cemite gestor da internet no brasil	global village telecom	EONBLUE	Thu Dec 22 22:49:58 GMT 2011	Sat May 05 10:35:58 GMT 2012
A	ns2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	cemite 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	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	cemite gestor da internet no brasil	global village telecom	EONBLUE	Wed Dec 21 04:27:57 GMT 2011	Wed Apr 25 04:52:02 GMT 2012
A	comeio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	18881	cemite 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	cemite 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	cemite gestor da internet no brasil	embratel	EONBLUE	Tue Sep 14 12:31:44 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	comeio2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite 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	cemite gestor da internet no brasil	embratel	EONBLUE	Thu Feb 11 19:15:47 GMT 2010	Mon Dec 19 19:40:43 GMT 2011
A	ns2.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	EONBLUE	Wed Sep 15 23:11:59 GMT 2010	Tue Dec 20 15:49:18 GMT 2011
A	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	EONBLUE	Thu Mar 03 19:37:08 GMT 2011	Tue Dec 20 15:49:18 GMT 2011
A	prodem.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	sv041.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	EONBLUE	Wed Feb 10 12:51:14 GMT 2010	Tue Sep 07 09:24:11 GMT 2010
A	comeio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	EONBLUE	Fri Feb 12 20:14:21 GMT 2010	Sat Dec 17 07:18:16 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Mon Jun 21 13:49:09 GMT 2010	Sat Nov 19 01:54:18 GMT 2011
A	comeio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	cemite gestor da internet no brasil	sepro	QUOVA	Thu Feb 19 20:37:04 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	comeio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	cemite 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	10954	cemite gestor da internet no brasil	sepro	QUOVA	Fri Mar 27 14:04:08 GMT 2009	Sat Nov 19 01:53:44 GMT 2011
A	teia.mme.gov.br	[REDACTED]	[REDACTED]	brazil	10954	cemite 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	cemite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	catalogo.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	webpac.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	prodem.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011
A	urano.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Tue May 19 11:27:09 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	teia.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite gestor da internet no brasil	embratel	QUOVA	Mon Apr 20 11:12:46 GMT 2009	Sat Nov 19 01:52:58 GMT 2011
A	comeio.mme.gov.br	[REDACTED]	[REDACTED]	brazil	4230	cemite 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	cemite gestor da internet no brasil	embratel	QUOVA	Mon May 03 15:09:41 GMT 2010	Sat Nov 19 01:52:58 GMT 2011

ANALYSIS – DISCOVER TARGET'S PROXY

Dynamic Configuration

Step name: Input IP ranges

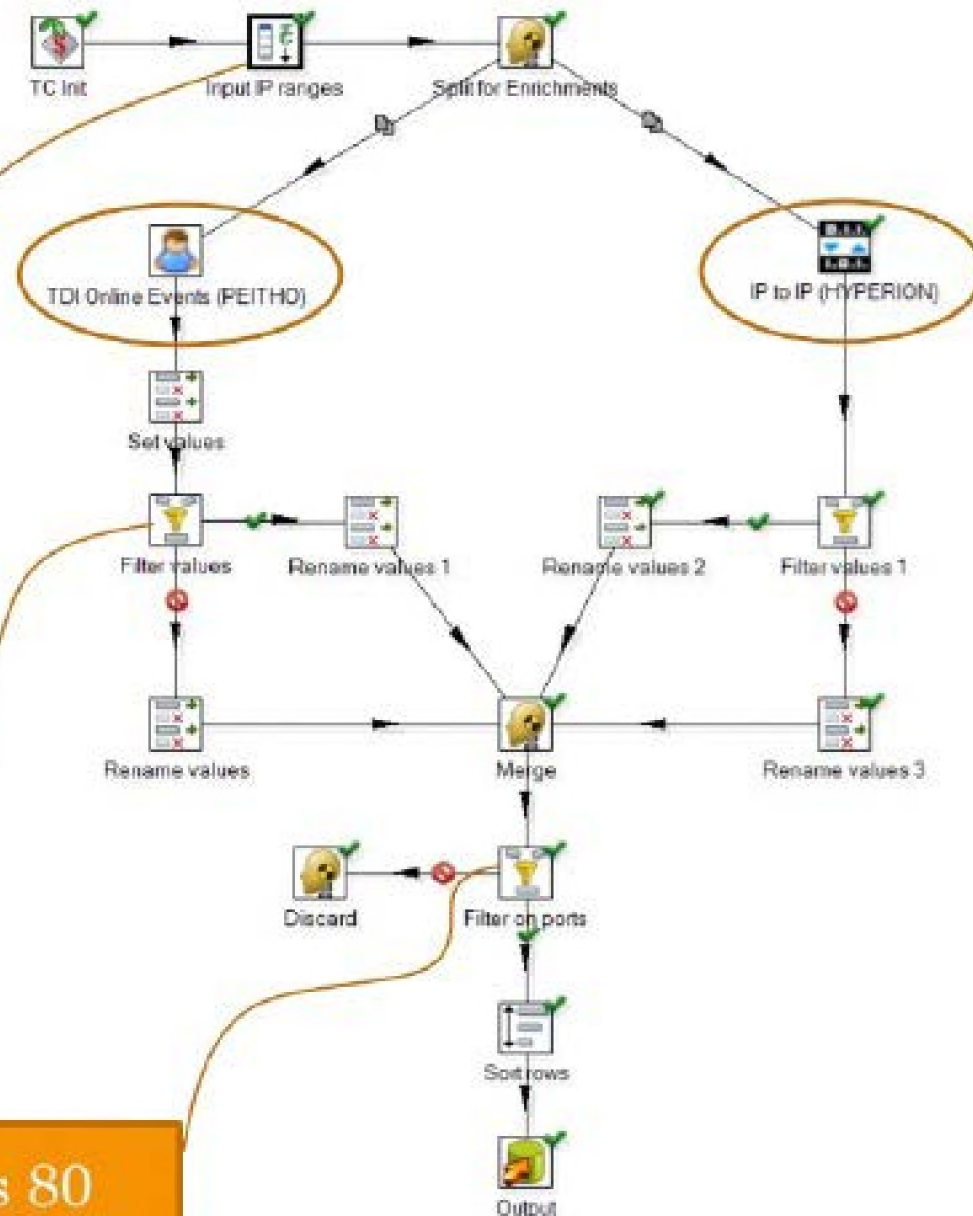
#	Config Name	Value	Default Value	Optional Value?	Field Name	Field Type
1	High IP	[REDACTED]		false	tc_highip	IP
2	IP Range	[REDACTED]		false	tc_iprange	iprange
3	Low IP	[REDACTED]		false	tc_lowip	IP

For more information, please go to [/tmp/peid/StepDynamic_Configuration](#)

OK Cancel

High IP
Low IP
IP Range

REMOTE PORT contains 80
REMOTE PORT contains 443



ANALYSIS – DISCOVER TARGET'S PROXY

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);6:483
[REDACTED]	[REDACTED]	6:443:TS (2);	6:54695:FC (1);6:435
[REDACTED]	[REDACTED]	6:443:TS (4);	6:31670:FC (1);6:343
[REDACTED]	[REDACTED]	6:443:TS (5);	6:1263:FC (1);6:4115
[REDACTED]	[REDACTED]	6:443:FS (12);	6:48927:TC (1);6:489
[REDACTED]	[REDACTED]	6:443:TS (179);6:80:1	6:26704:FC (1);6:267
[REDACTED]	[REDACTED]	6:443:TS (1);	6:11217:FC (1);
[REDACTED]	[REDACTED]	6:443:TS (165);	6:12946:FC (1);6:152
[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	6:39170:FC (2);6:536

Entity IP :

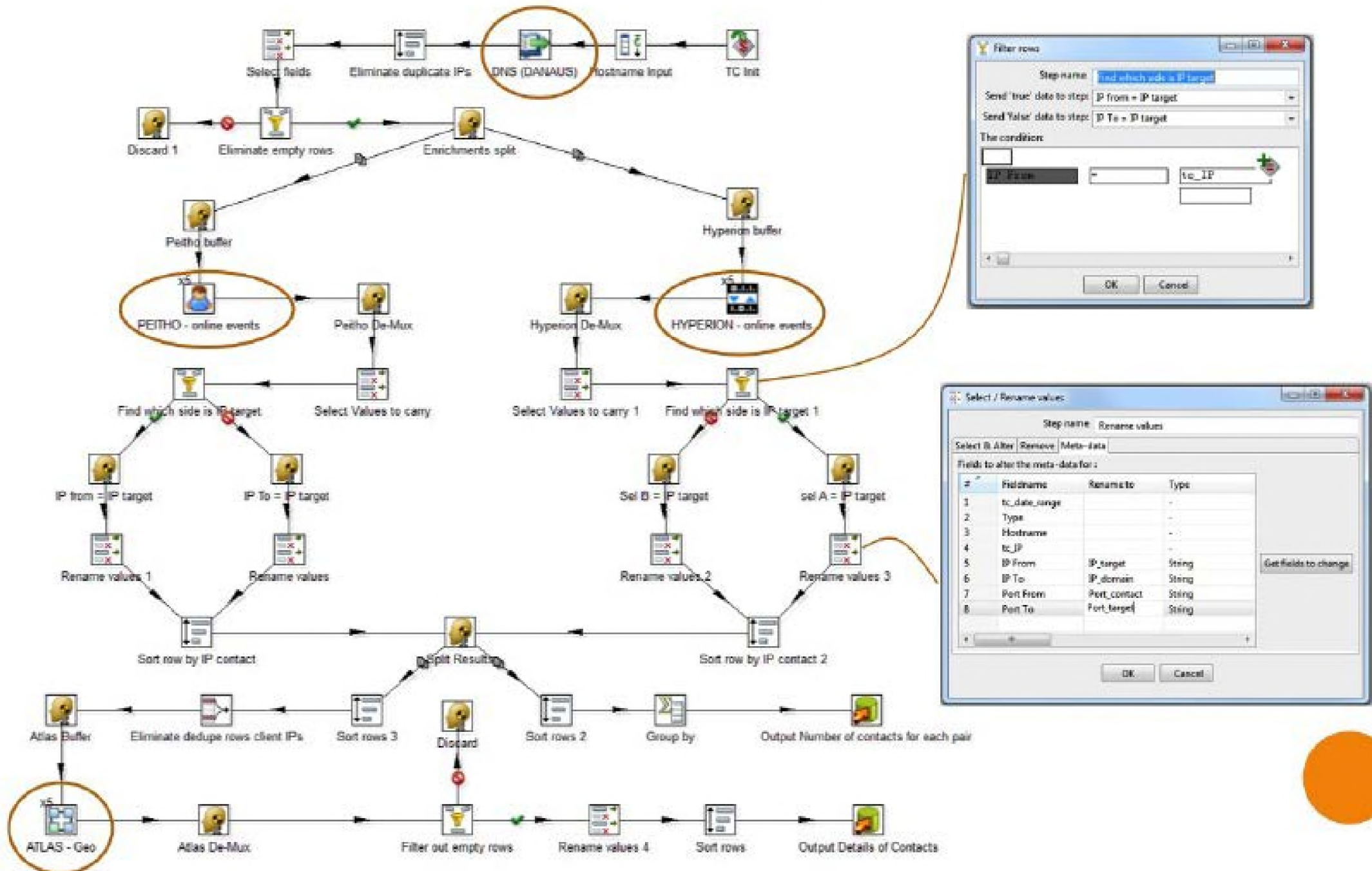
Remote IP : various

Remote Port : 443

Entity Port: various



ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH



ANALYSIS – DETERMINE IPs MY TARGET COMMUNICATES WITH

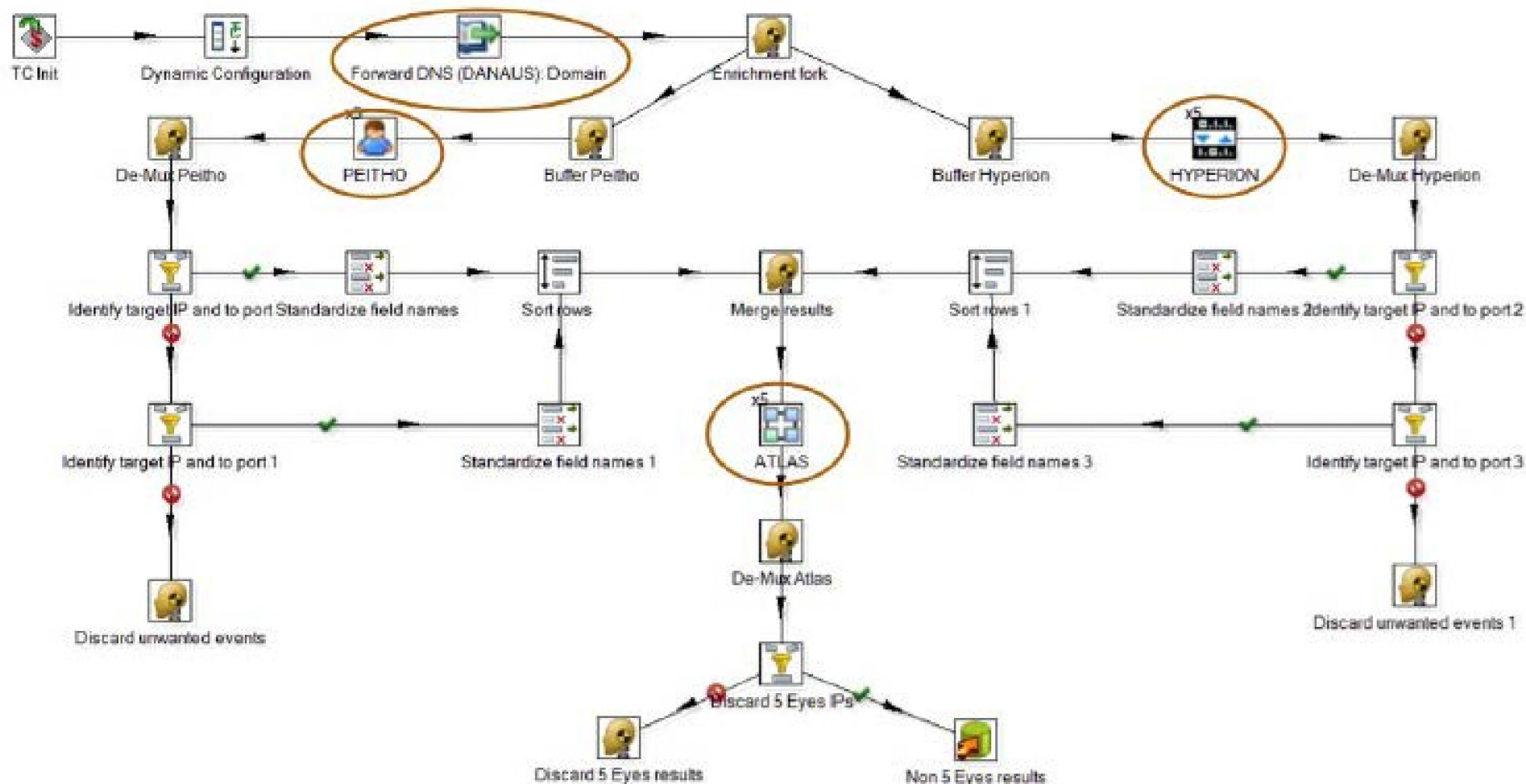
Hostname domain	IP domain	IP in contact with domain	Port used by IP domain	Port used by IP contact	Owner of IP contact	Carrier of IP contact	ASN of IP contact	Country of IP contact	IP range for IP contact
correio.mme.gov.br			6-25/T3 (1);	6-61391:FC (1);	tse i net noc ip infrastructure	british telecommunications plc	5400 eritrea		
correio.mme.gov.br			6-25/T3 (1);	6-61351:FC (1);	tse i net noc ip infrastructure	british telecommunications plc	5400 eritrea		
correio.mme.gov.br			6-25/T3 (2);6-25/F5 (1);	6-34251:FC (2)	tata communications	tata communications	6453 canada		
correio.mme.gov.br			6-25/T3 (1);	6-28151:FC (1);	jtc	jordan telecommunications com	8697 jordan		
correio.mme.gov.br			6-25/T3 (1);	6-2990:FC (1);	reassign to idc-dbw-idc customers for info public company limite		9891 thailand		
correio.mme.gov.br			6-25/F5 (1);	6-50072:TC (1);	internal network	international data exchange llc	12534 jordan		
correio.mme.gov.br			6-25/T3 (1);	6-51934:FC (1);	parsonline	parsonline	16322 iran		
correio.mme.gov.br			6-25/T3 (1);	6-2295:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25/T3 (1);	6-1796:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25/T3 (1);	6-50329:FC (1);	dsl home subscribers	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-25/T3 (1);	6-22433:FC (1);	saudnet saudi telecom compon	saudnet	25019 saudi arabia		
correio.mme.gov.br			6-54156:TC	6-25/F5 (128);	iweb dedicated hd	iweb technologies inc.	32613 canada		
correio.mme.gov.br			6-33907:TC	6-25/F5 (22);	iweb dedicated hd	iweb technologies inc.	32613 canada		
correio.mme.gov.br			6-25/T3 (4);	6-57773:FC	middle east internet company llc/cyberia ri yadh		34397 saudi arabia		
www.mme.gov.br			6-80/F5 (1);	6-54791:TC (1);	adsl service	sahara net	41176 saudi arabia		

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

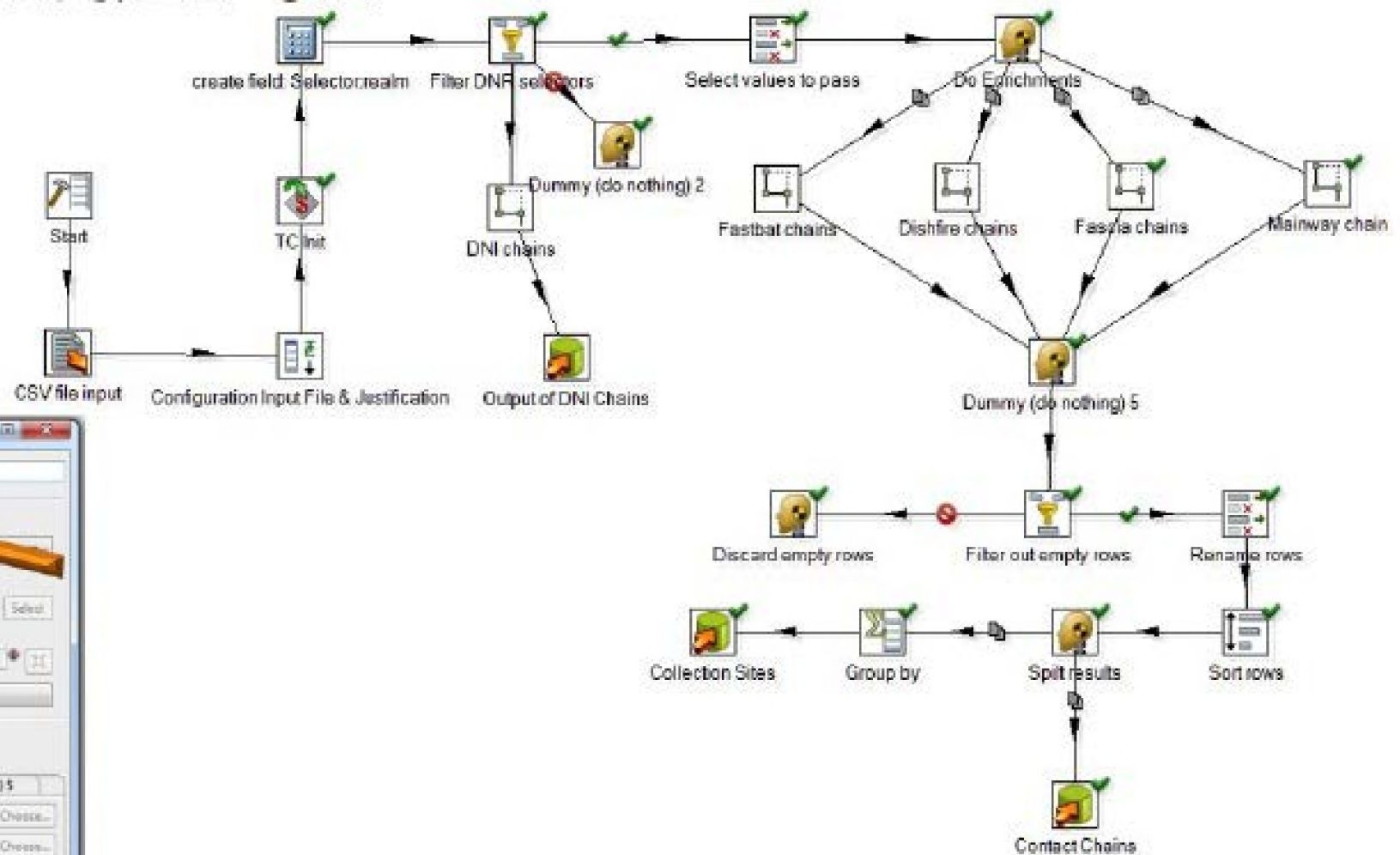
target_hostname	target	contact	target_port	contact_port	Case Notations	Country	Digraph
acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	6:41278:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br
acessovpn.mme.gov.br	[REDACTED]	[REDACTED]	6:30141:TC (1);	6:80:FS (1);	MA10099 (1);	brazil	br

ASN contact	Country contact	# IPs contact
18881	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
18881	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

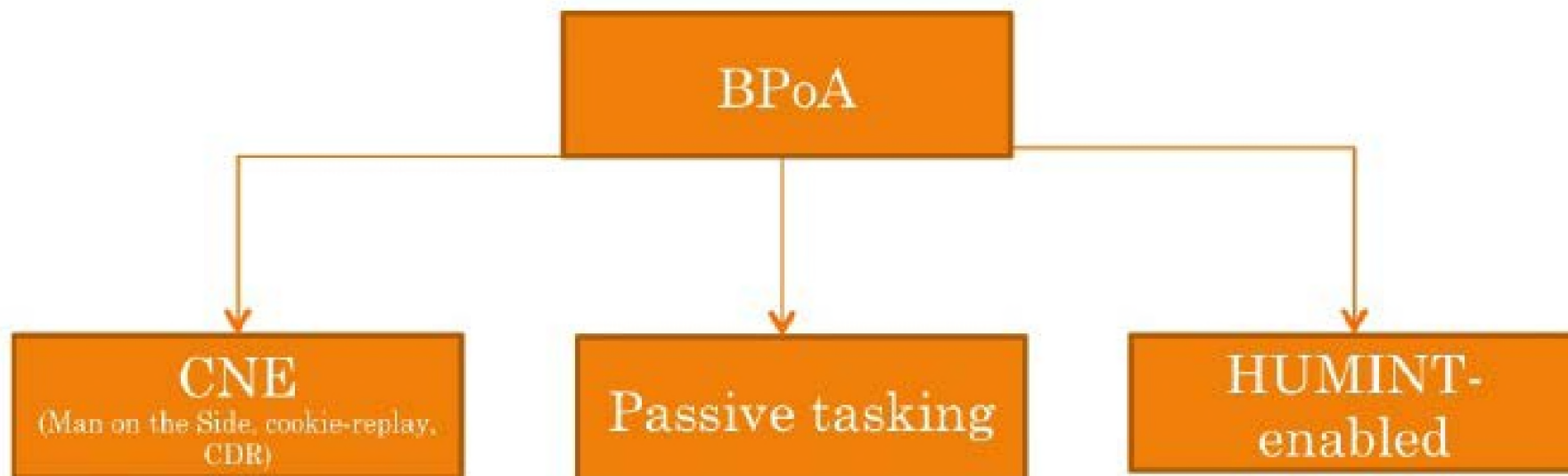
Source	Type	Hostname	Hostname Decoded	IPs
EONBLUE	A	wwwnet.net.br	wwwnet.net.br	[REDACTED]
EONBLUE	A	stoughtn.com.br	stoughtn.com.br	[REDACTED]
EONBLUE	A	transformadosecuras.com.br	transformadosecuras.com.br	[REDACTED]
EONBLUE	A	geofreder.br	geofreder.br	[REDACTED]
EONBLUE	A	maylras.com.br	maylras.com.br	[REDACTED]
EONBLUE	A	fatecfeq.edu.br	fatecfeq.edu.br	[REDACTED]
EONBLUE	A	abclor.com.br	abclor.com.br	[REDACTED]
EONBLUE	A	feletrived.org.br	feletrived.org.br	[REDACTED]
EONBLUE	A	afablog.com.br	afablog.com.br	[REDACTED]
EONBLUE	A	edvcc.com.br	edvcc.com.br	[REDACTED]
EONBLUE	A	metajato.com.br	metajato.com.br	[REDACTED]
EONBLUE	A	guriatons.com.br	guriatons.com.br	[REDACTED]
EONBLUE	A	atag.com.br	atag.com.br	[REDACTED]
EONBLUE	A	flitepress.com.br	flitepress.com.br	[REDACTED]
EONBLUE	A	mhrvagens.com.br	mhrvagens.com.br	[REDACTED]
EONBLUE	A	stephendot.com.br	stephendot.com.br	[REDACTED]
EONBLUE	A	2housesmoves.com.br	2housesmoves.com.br	[REDACTED]
EONBLUE	A	thats.com.br	thats.com.br	[REDACTED]
EONBLUE	A	getna.com.br	getna.com.br	[REDACTED]
EONBLUE	A	edpoh.com.br	edpoh.com.br	[REDACTED]
EONBLUE	A	institutopec.org	institutopec.org	[REDACTED]

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.

