SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Elegant CHAOS

Project Leads: [redacted]

Code Support: [redacted]

For more up-to-date information please visit this URL:
[redacted] Elegant_Chaos
For recent developments please contact the authors.

[redacted]

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Small team = faster development

Specialities:

[redacted]: project vision, keeping on track with partner sharing and end-to-end automation goals

[redacted]: project vision, MySQL support, analytic perspective

[redacted]: project organization, Whizbang/Cloudbase development, developers perspective

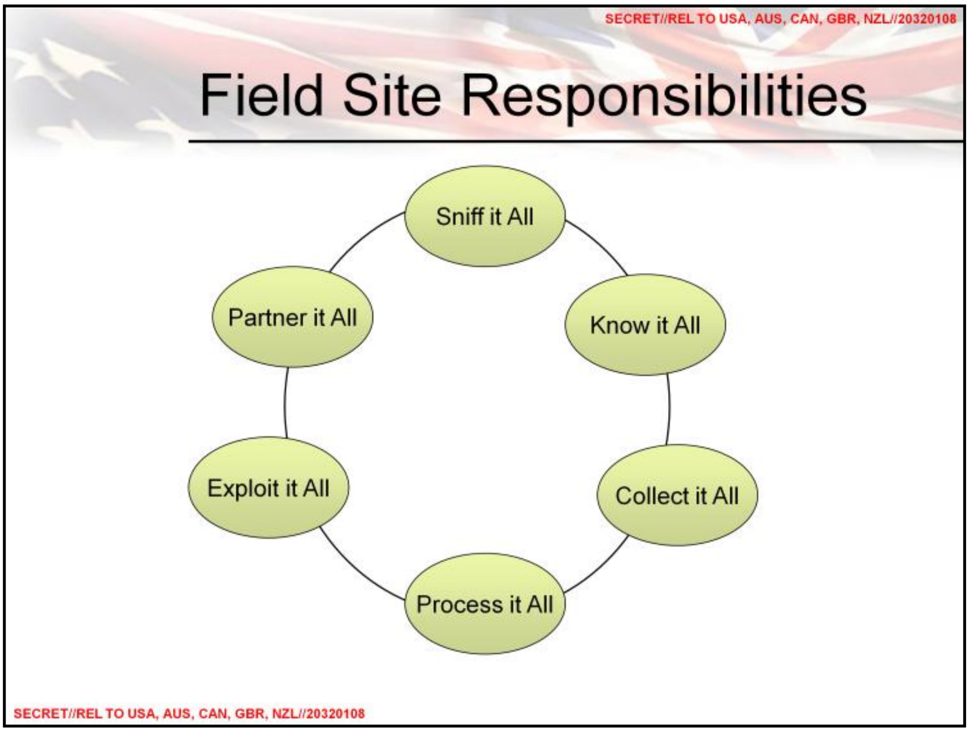
[redacted]: code support for new data flows, MySQL, Whizbang development

Other contributors:

Cloud Support Team

[redacted]

[redacted]



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Field Site Responsibilities

Sniff it All

Know it All

Collect it All

Process it All

Exploit it All

Partner it All

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Sniff it all: Maximize receiving capabilities within our viewing arc

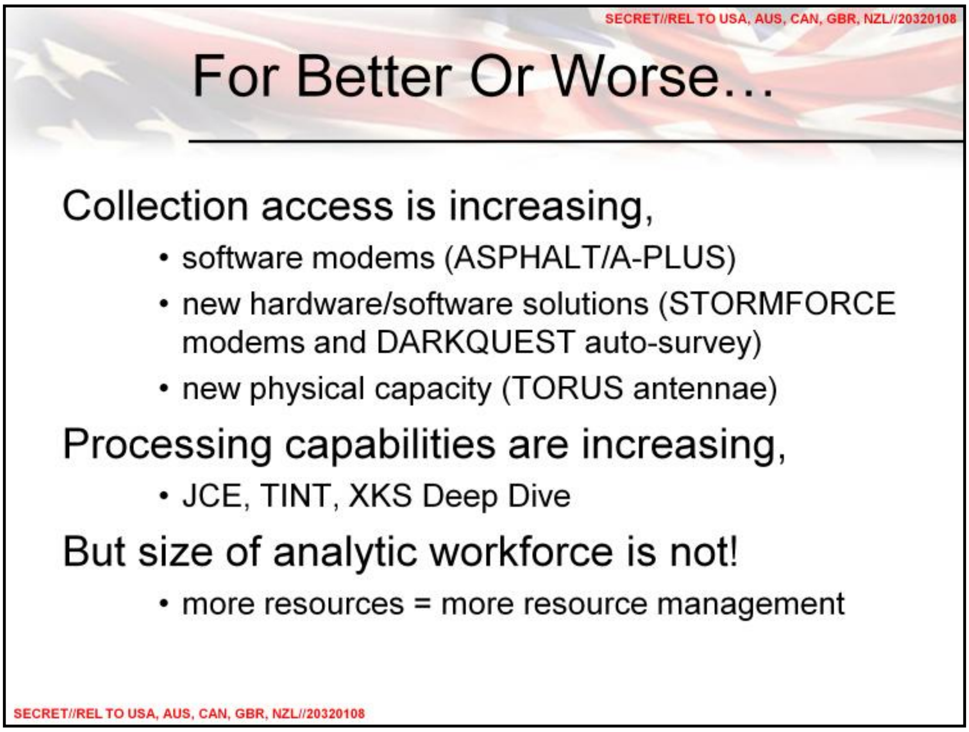
Know it all: Survey enough to keep our finger on the pulse of the whole environment

Collect it all: Maximize how many signals we can bring in the door simultaneously

Process it all: Find the data in the signal

Exploit it all: Find the intelligence in the signal

Partner it all: Collaborate on techniques and share data with partners



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

For Better Or Worse…

Collection access is increasing,

- software modems (ASPHALT/A-PLUS)
- new hardware/software solutions (STORMFORCE modems and DARKQUEST auto-survey)
- new physical capacity (TORUS antennae)

Processing capabilities are increasing,

- JCE, TINT, XKS Deep Dive

But size of analytic workforce is not!

- more resources = more resource management

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

We have about 9100 signals in our view

In 2008, we were only processing maybe 100-140 of these

Director's edict to "collect it all"

ASPHALT -> software modems processing low bit rate signals added a 300-signal capability

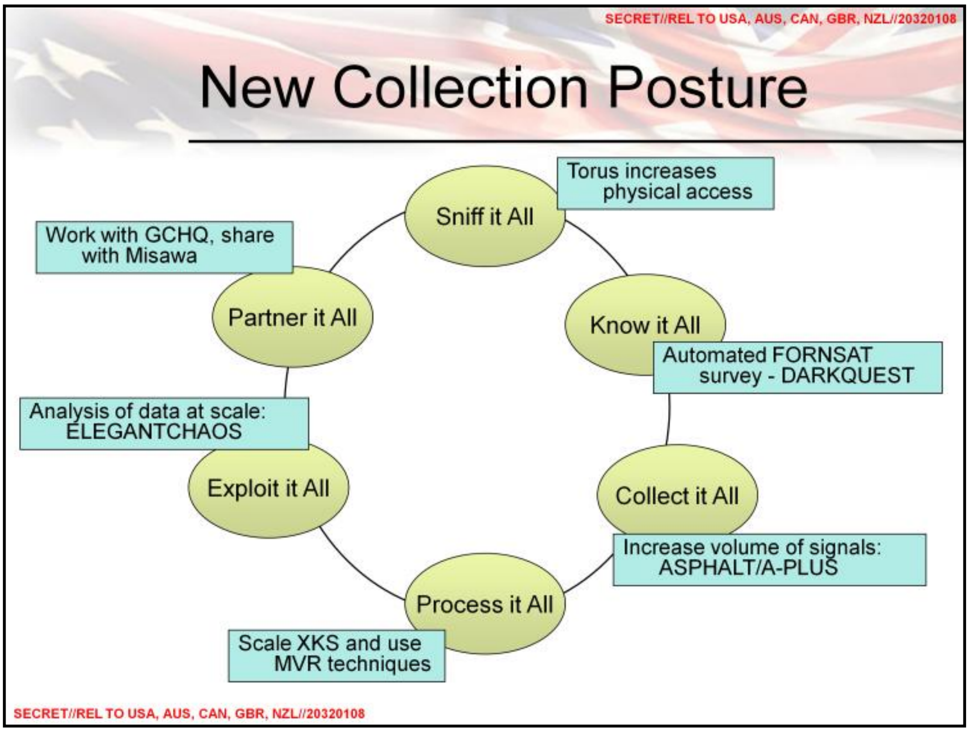
STORMFORCE modems -> combination of hardware and software control increase capacity from 4 signals to 40

TORUS antenna -> 12 receivers (feeds) in place of 1

Now we are at ~500, moving quickly towards 1,000

Over the next year, we anticipate collecting 3,000 signals simultaneously

When a resource comes available, which signal do you place on collection???



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

New Collection Posture

Sniff it All

Torus increases physical access

Know it All

Automated FORNSAT survey - DARKQUEST

Collect it All

Increase volume of signals: ASPHALT/A-PLUS

Process it All

Scale XKS and use MVR techniques

Exploit it All

Analysis of data at scale: ELEGANTCHAOS

Partner it All

Work with GCHQ, share with Misawa

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Sniff it all: TORUS adds 12 new feeds to existing 20-some

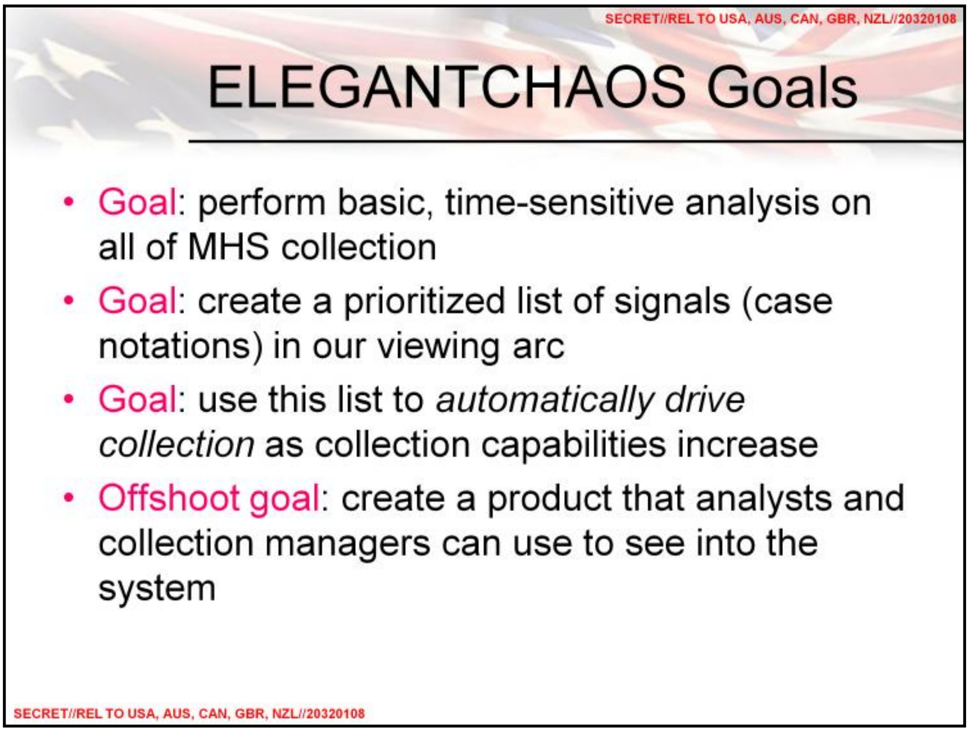
Know it all: DARKQUEST COMSAT development automates survey to capture all signals, at MHS, in a 2-week span.

Collect it all: Increased modem capacity with software (APLUS) & STORMFORCE modems.

Process it all: Scale XKS, consider Deep Dive XKS, use MVR techniques such as map/reduce and Cloudbase capabilities

Exploit it all: Query focused datasets - Analysis of data at scale means automate, automate, automate. This is the motivation for ELEGANTCHAOS. Optimize automation to include: automate scoring of links based on current analytical priorities, and feeding prioritized list back to survey tools including DARKQUEST and modems. Secondary goals: transparent process; flexible scoring.

Partner it all: Collaborate on techniques and share data with partners. Cloud solution = TINT; XKS scaling = JCE. First partner: GCHQ/Bude.

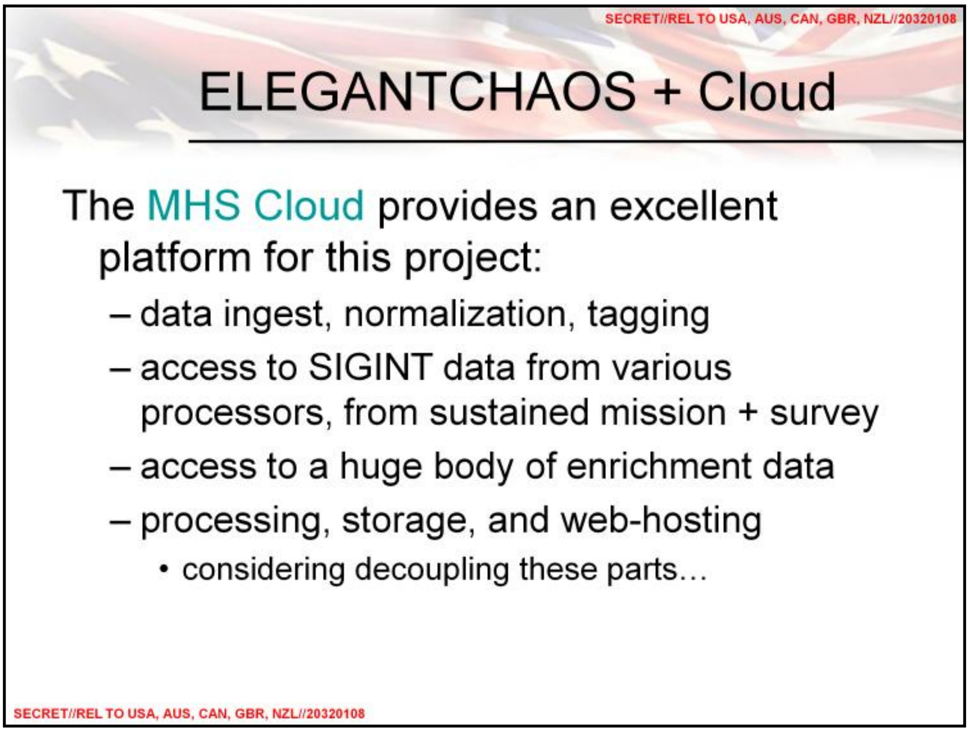


SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

ELEGANTCHAOS Goals

- Goal: perform basic, time-sensitive analysis on all of MHS collection
- Goal: create a prioritized list of signals (case notations) in our viewing arc
- Goal: use this list to *automatically drive collection* as collection capabilities increase
- Offshoot goal: create a product that analysts and collection managers can use to see into the system

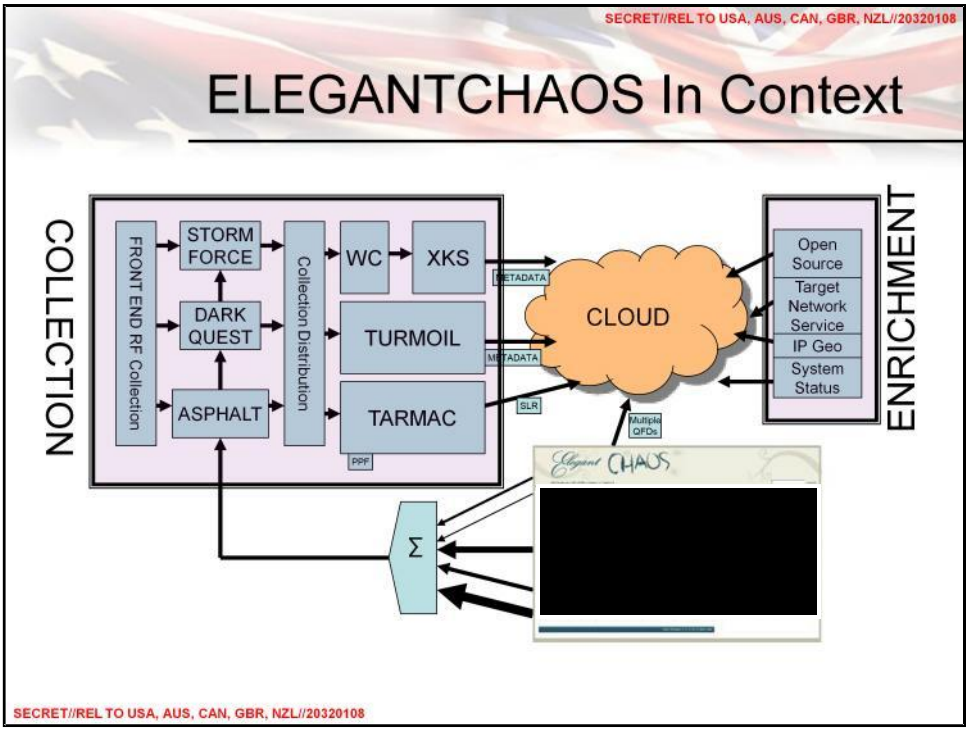
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



ELEGANTCHAOS + Cloud

The MHS Cloud provides an excellent platform for this project:

- data ingest, normalization, tagging
- access to SIGINT data from various processors, from sustained mission + survey
- access to a huge body of enrichment data
- processing, storage, and web-hosting
  - considering decoupling these parts…



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

ELEGANTCHAOS In Context

[redacted]

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

TARMAC provides target activity, network space,

XKS provides target activity, network space, technologies

POPQUIZ provides malicious discovery across sessions using heuristic-type approaches.

Flexibility in terms of

QFD’s: derived from XKS, SLR, Popquiz, etc.

Target activity

Technology

Geo-location

Questions: can combine QFDs

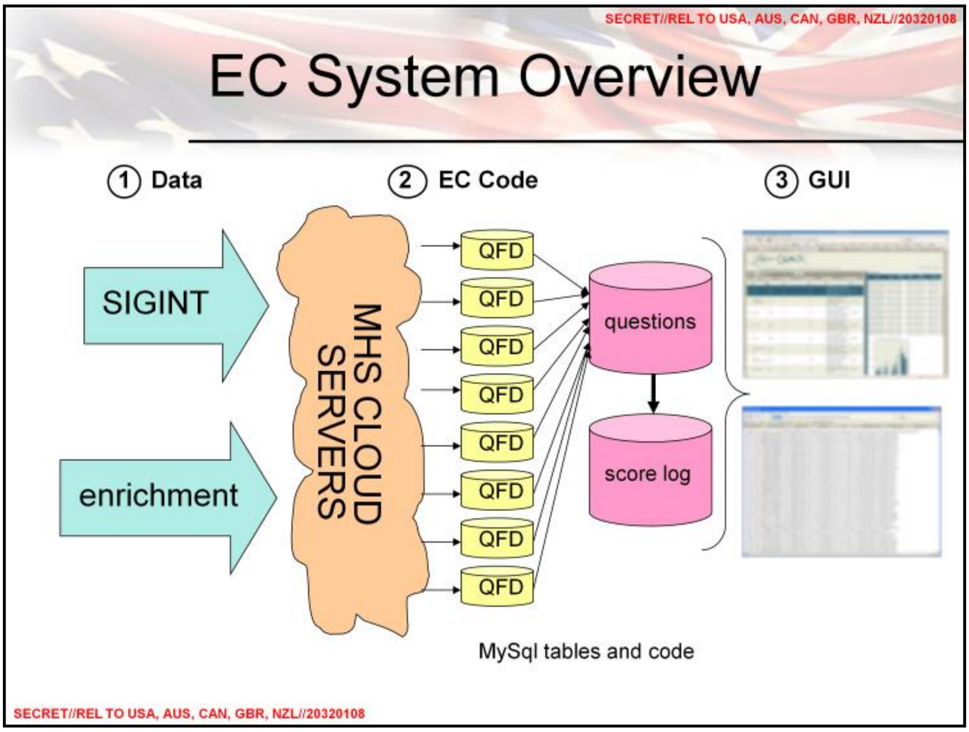
VPNs involving Ivory Coast?

Paired links carrying VOIP or VPN?

Malicious Activity on networks used by targets?

Experiment by doing

Will challenge current tasking methods, hopefully make them easier ;-)



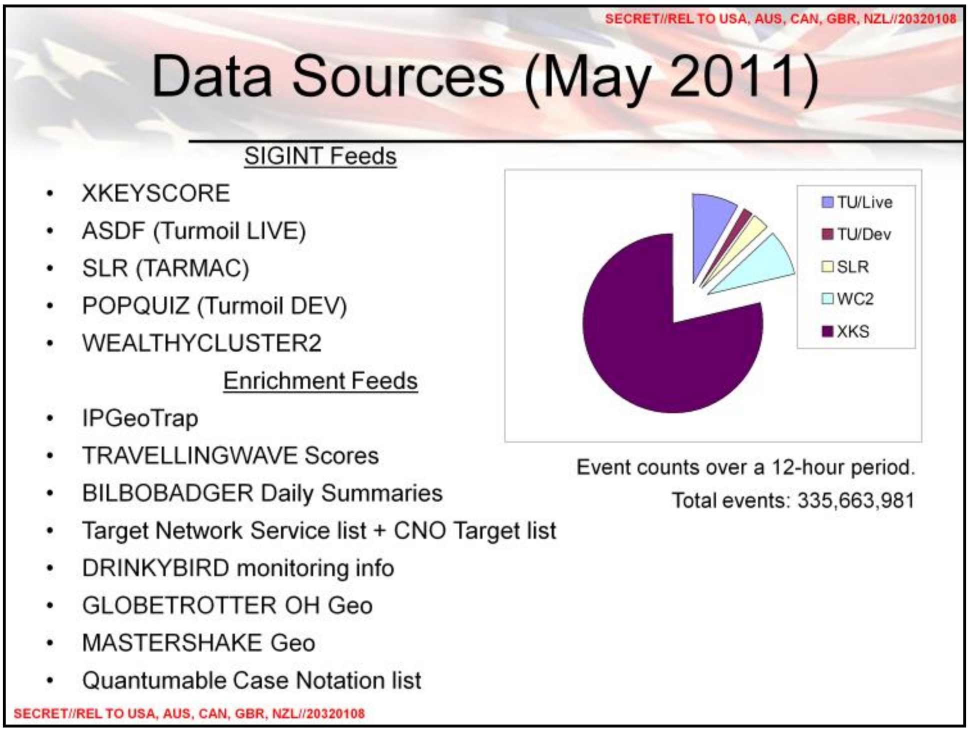
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

EC System Overview

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

This is a simplified view of the ELEGANTCHAOS machinery. **Note: a key component that is not shown is the feedback loop into collection.**

1) SIGINT and enrichment data enters the system by being copied to the Cloud servers. This may take the form of a MAILORDER flow, a wget grab, or a database file transfer from another system.
2) Data is processed. Some data is processed through the SIGDEV Cloud Stack, which formally validates/normalizes/tags the data. All SIGINT data goes through this process, as well as some of the enrichment data. The remaining enrichment data usually requires some minimal processing or reformatting.
3) The results of step 2, whether pulled from the SIGDEV Cloud Stack via the WhizBang map/reduce API, or copied from an external source, are stored in Question Focused Datasets (QFDs). Some QFDs serve multiple analytic interests, and some analytic interests require an intersection of QFDs to evaluate.
4) ELEGANTCHAOS MySql code pulls analytical questions from a database, queries the QFDs to find case notations satisfying each question, and writes scores to another database. These scoring databases at the heart of EC populate the GUI.



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Data Sources (May 2011)

SIGINT Feeds

- XKEYSCORE
- ASDF (Turmoil LIVE)
- SLR (TARMAC)
- POPQUIZ (Turmoil DEV)
- WEALTHYCLUSTER2

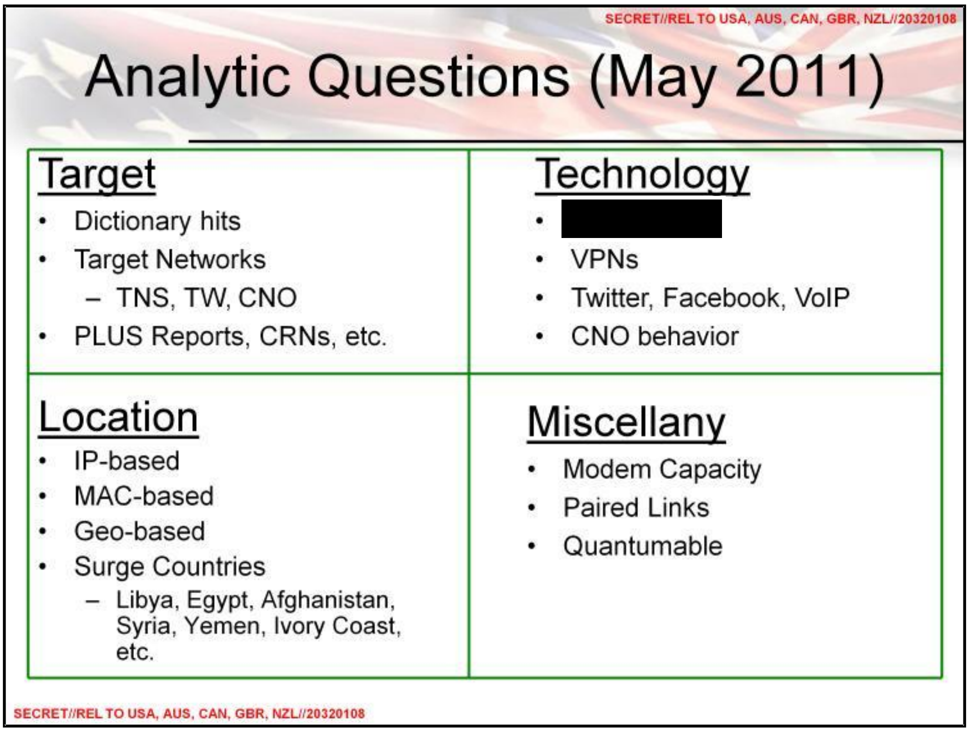
Enrichment Feeds

- IPGeoTrap
- TRAVELLINGWAVE Scores
- BILBOBADGER Daily Summaries
- Target Network Service list + CNO Target list
- DRINKYBIRD monitoring info
- GLOBETROTTER OH Geo
- MASTERSHAKE Geo
- Quantumable Case Notation list

Event counts over a 12-hour period.

Total events: 335,663,981

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Analytic Questions (May 2011)

Target

- Dictionary hits
- Target Networks
  - TNS, TW, CNO
- PLUS Reports, CRNs, etc.

Technology

- [redacted]
- VPNs
- Twitter, Facebook, VoIP
- CNO behavior

Location

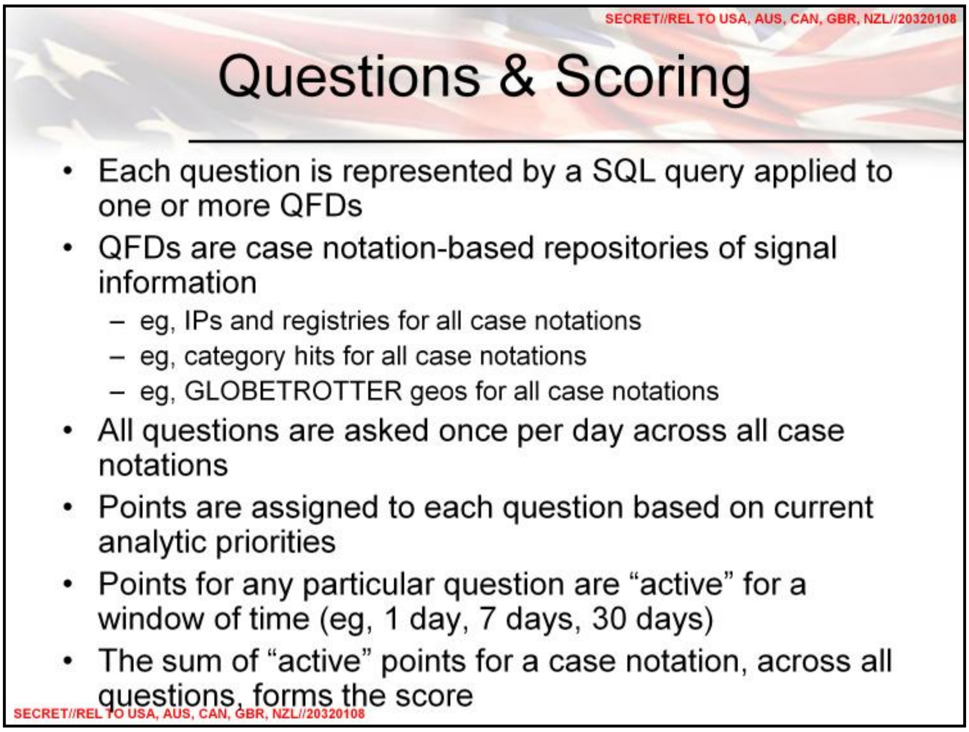
- IP-based
- MAC-based
- Geo-based
- Surge Countries
  - Libya, Egypt, Afghanistan, Syria, Yemen, Ivory Coast, etc.

Miscellany

- Modem Capacity
- Paired Links
- Quantumable

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Don’t forget combinations (paired links with VPNs, VPNs with target IP networks)

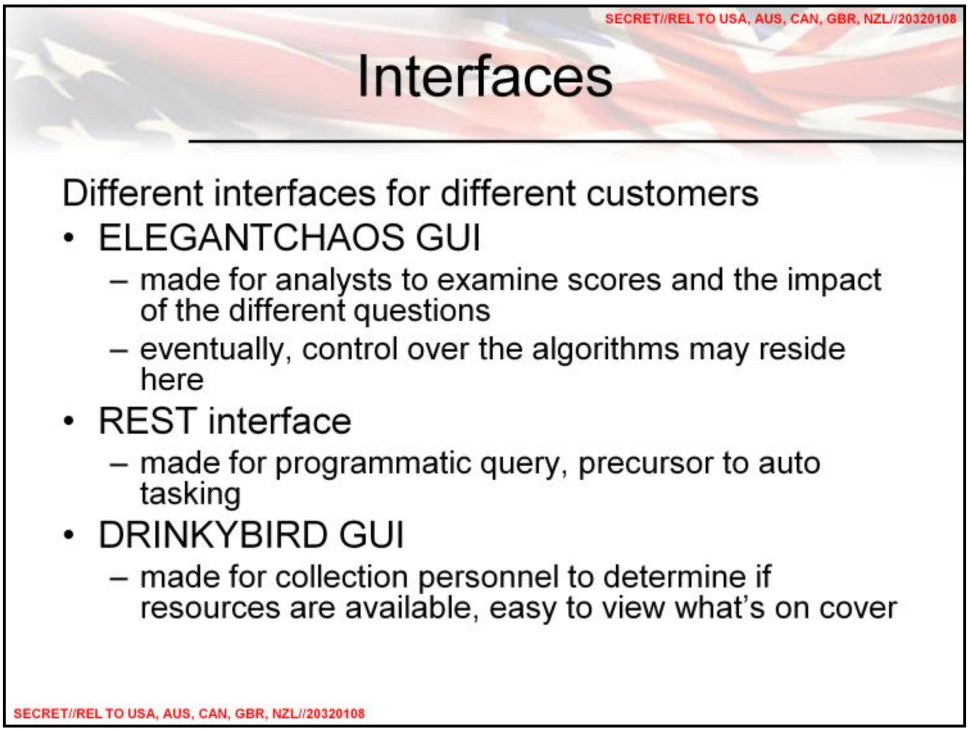


SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Questions & Scoring

- Each question is represented by a SQL query applied to one or more QFDs
- QFDs are case notation-based repositories of signal information
  - eg, IPs and registries for all case notations
  - eg, category hits for all case notations
  - eg, GLOBETROTTER geos for all case notations
- All questions are asked once per day across all case notations
- Points are assigned to each question based on current analytic priorities
- Points for any particular question are “active” for a window of time (eg, 1 day, 7 days, 30 days)
- The sum of “active” points for a case notation, across all questions, forms the score

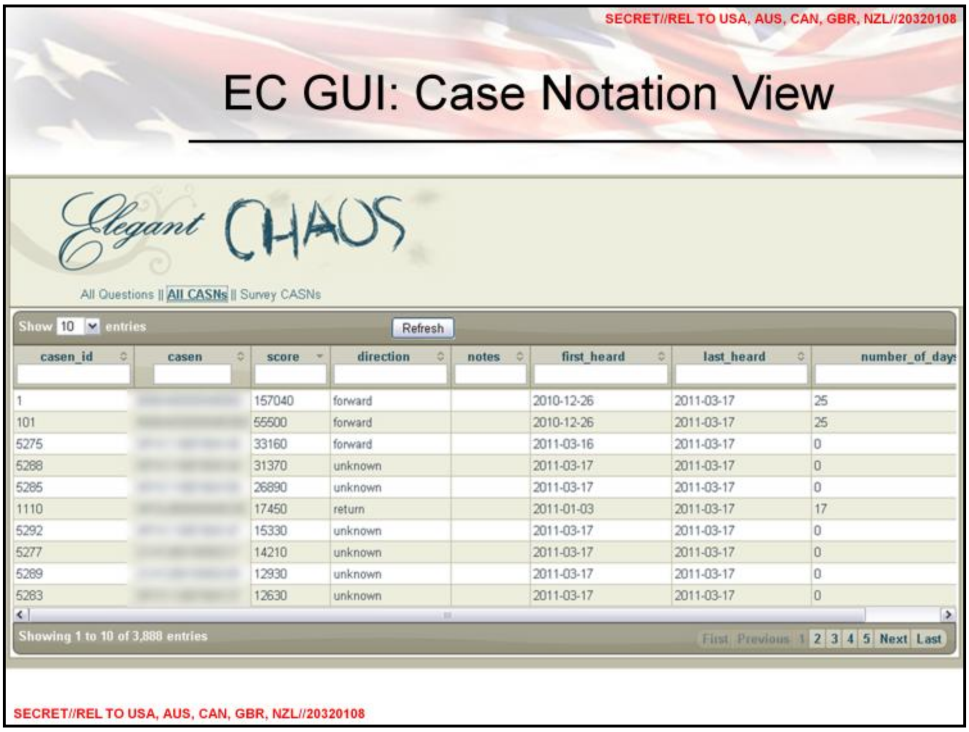
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



Interfaces

Different interfaces for different customers

- ELEGANTCHAOS GUI
  - made for analysts to examine scores and the impact of the different questions
  - eventually, control over the algorithms may reside here
- REST interface
  - made for programmatic query, precursor to auto tasking
- DRINKYBIRD GUI
  - made for collection personnel to determine if resources are available, easy to view what’s on cover



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

EC GUI: Case Notation View

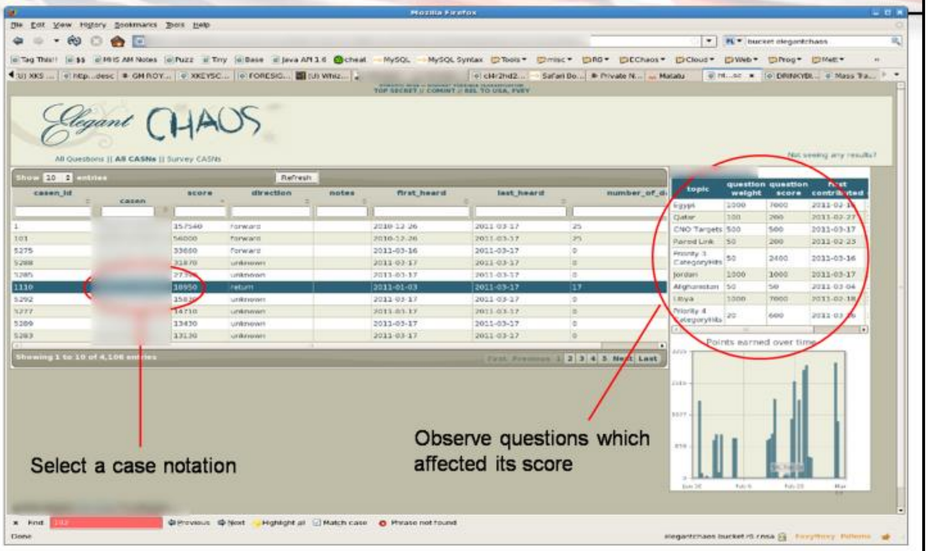
casen_id	casen	score	direction	notes	first_heard	last_heard	number_of_days
1	[redacted]	157040	forward		2010-12-26	2011-03-17	25
101	[redacted]	55500	forward		2010-12-26	2011-03-17	25
5275	[redacted]	33160	forward		2011-03-16	2011-03-17	0
5288	[redacted]	31370	unknown		2011-03-17	2011-03-17	0
5285	[redacted]	26890	unknown		2011-03-17	2011-03-17	0
1110	[redacted]	17450	return		2011-01-03	2011-03-17	17
5292	[redacted]	15330	unknown		2011-03-17	2011-03-17	0
5277	[redacted]	14210	unknown		2011-03-17	2011-03-17	0
5289	[redacted]	12930	unknown		2011-03-17	2011-03-17	0
5283	[redacted]	12630	unknown		2011-03-17	2011-03-17	0

Showing 1 to 10 of 3,888 entries

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Continual assessment of bearers helps to determine when a bearer becomes less interesting, then it'd be possible to remove it from sustained collection.

EC GUI: Case Notation View



Mozilla Firefox
File Edit View History Bookmarks Tools Help
Tag This!! $$ MHS AM Notes Puzz Tiny Base Java API 1.6 cheat MySQL MySQL Syntax Tools misc RG ECChaos Cloud Web Prog Met
(U) XKS ... http...desc GM ROY... XKEYSC... FORESIG... (U) Whiz... cl4r2hd2... Safari Bo... Private N... Matatu DRINKYBI... Mass Tra...
TOP SECRET // COMINT // REL TO USA, FVEY
Elegant CHAOS
All Questions || All CASNs || Survey CASNs
Not seeing any results?
Show 10 entries
Refresh
Showing 1 to 10 of 4,106 entries
First Previous 1 2 3 4 5 Next Last
Points earned over time
Find
Previous Next Highlight all Match case Phrase not found
Done

casen_id	casen	score	direction	notes	first_heard	last_heard	number_of_d
1	[redacted]	157540	forward		2010-12-26	2011-03-17	25
101	[redacted]	56000	forward		2010-12-26	2011-03-17	25
5275	[redacted]	33660	forward		2011-03-16	2011-03-17	0
5288	[redacted]	31870	unknown		2011-03-17	2011-03-17	0
5285	[redacted]	27[illegible]	unknown		2011-03-17	2011-03-17	0
1110	[redacted]	18950	return		2011-01-03	2011-03-17	17
5292	[redacted]	158[illegible]	unknown		2011-03-17	2011-03-17	0
5277	[redacted]	14710	unknown		2011-03-17	2011-03-17	0
5289	[redacted]	13430	unknown		2011-03-17	2011-03-17	0
5283	[redacted]	13130	unknown		2011-03-17	2011-03-17	0

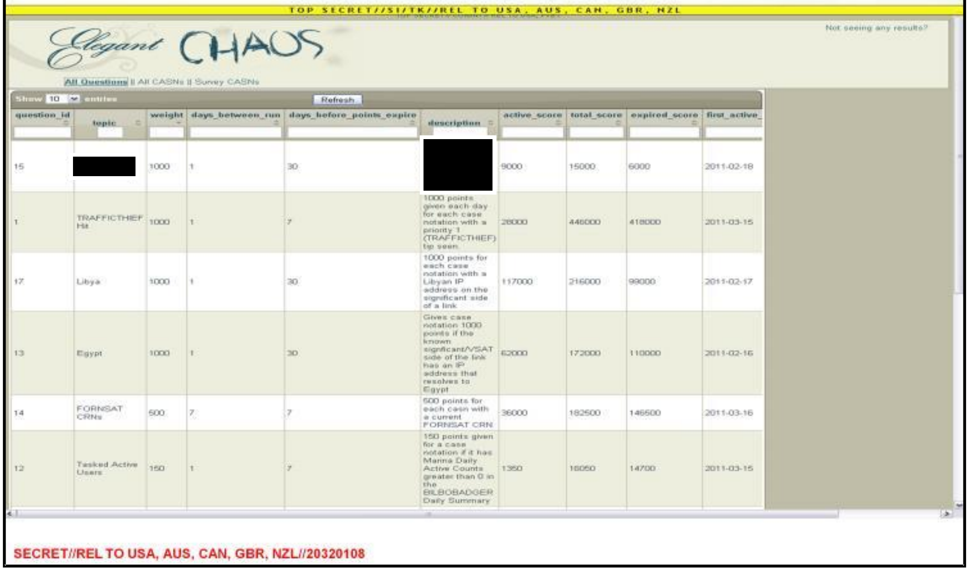
topic	question weight	question score	first contributed
Egypt	1000	7000	2011-02-1[illegible]
Qatar	100	200	2011-02-27
CNO Targets	500	500	2011-03-17
Paroid Link	50	200	2011-02-23
Priority 3 CategoryHits	50	2400	2011-03-16
Jordan	1000	1000	2011-03-17
Afghanistan	50	50	2011-03-04
Libya	1000	7000	2011-02-18
Priority 4 CategoryHits	20	600	2011-03-[illegible]

Select a case notation

Observe questions which affected its score

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

EC GUI: Question View



TOP SECRET//SI/TK//REL TO USA, AUS, CAN, GBR, NZL

question_id	topic	weight	days_between_run	days_before_points_expire	description	active_score	total_score	expired_score	first_active_
15	[redacted]	1000	1	30	[redacted]	9000	15000	6000	2011-02-18
1	TRAFFICTHIEF Hit	1000	1	7	1000 points given each day for each case notation with a priority 1 (TRAFFICTHIEF) tip seen.	28000	446000	418000	2011-03-15
17	Libya	1000	1	30	1000 points for each case notation with a Libyan IP address on the significant side of a link	117000	216000	99000	2011-02-17
13	Egypt	1000	1	30	Gives case notation 1000 points if the known significant/VSAT side of the link has an IP address that resolves to Egypt	62000	172000	110000	2011-02-16
14	FORNSAT CRNs	500	7	7	500 points for each casn with a current FORNSAT CRN	36000	182500	146500	2011-03-16
12	Tasked Active Users	150	1	7	150 points given for a case notation if it has Marina Daily Active Counts greater than 0 in the BILBOBADGER Daily Summary	1350	16050	14700	2011-03-15

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Important to remember, this is our attempt to best utilize increasing capacity. Sits between sustained/CRN collection and continual survey.

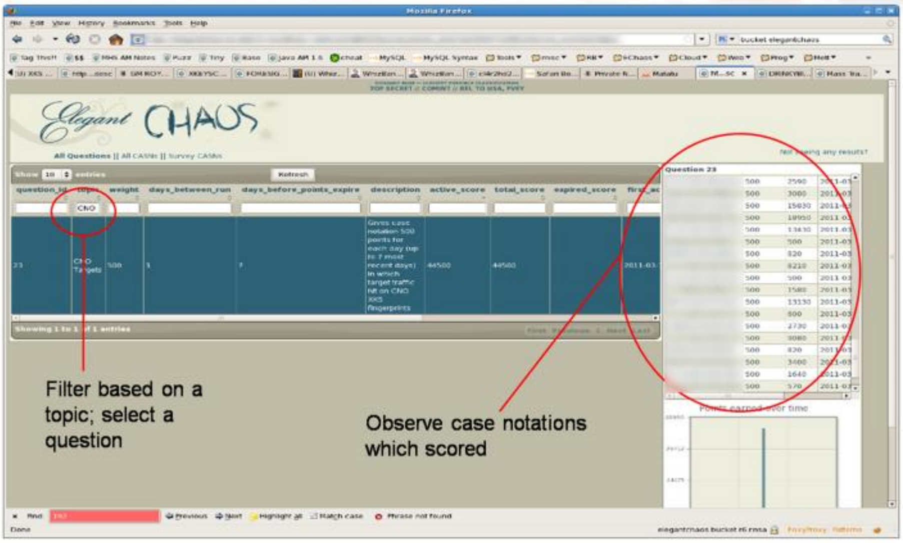
Provides ability to turn the dials on “hot topic” of the day.

Can adjust the length of time an event remains interesting and affects prioritization.

Some Questions will always be run. TT hit, confirmed target activity, [redacted], etc.

Maintains history, so progress can be tracked. Are there more target hits, [redacted], paired VOIP signals, etc.

EC GUI: Question View


Mozilla Firefox
TOP SECRET // COMINT // REL TO USA, FVEY
Elegant CHAOS
All Questions || All CASNs || Survey CASNs
Show 10 entries
Refresh
Not seeing any results?
Showing 1 to 1 of 1 entries
First Previous 1 Next Last
Points earned over time
Previous Next Highlight all Match case Phrase not found
Done
elegantchaos bucket r6 rmsa

question_id	topic	weight	days_between_run	days_before_points_expire	description	active_score	total_score	expired_score	first_ac
	CNO								
23	CNO Targets	500	1	7	Gives case notation 500 points for each day (up to 7 most recent days) in which target traffic hit on CNO XKS fingerprints	44500	44500		2011-03

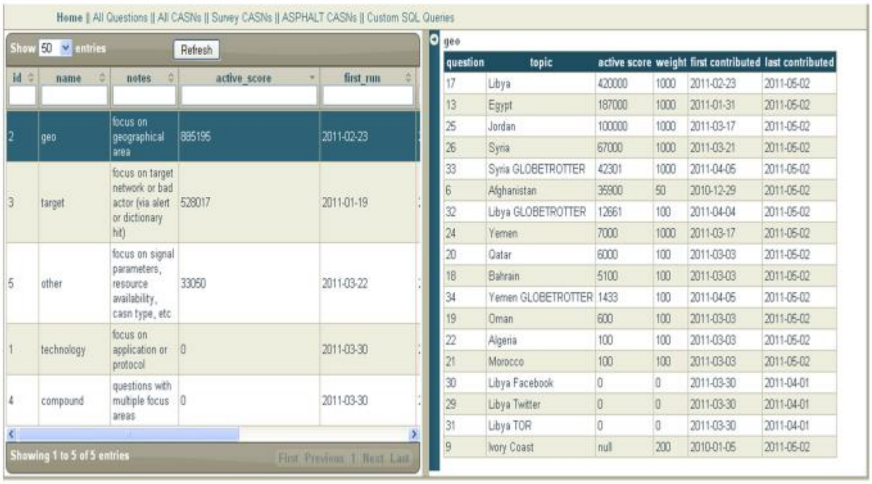
Question 23

[redacted]	500	2590	2011-03
[redacted]	500	3000	2011-03
[redacted]	500	15030	2011-03
[redacted]	500	18950	2011-03
[redacted]	500	13430	2011-03
[redacted]	500	500	2011-03
[redacted]	500	820	2011-03
[redacted]	500	8210	2011-03
[redacted]	500	500	2011-03
[redacted]	500	1580	2011-03
[redacted]	500	13130	2011-03
[redacted]	500	600	2011-03
[redacted]	500	2730	2011-03
[redacted]	500	3080	2011-03
[redacted]	500	820	2011-03
[redacted]	500	3400	2011-03
[redacted]	500	1640	2011-03
[redacted]	500	570	2011-03

Filter based on a topic; select a question

Observe case notations which scored

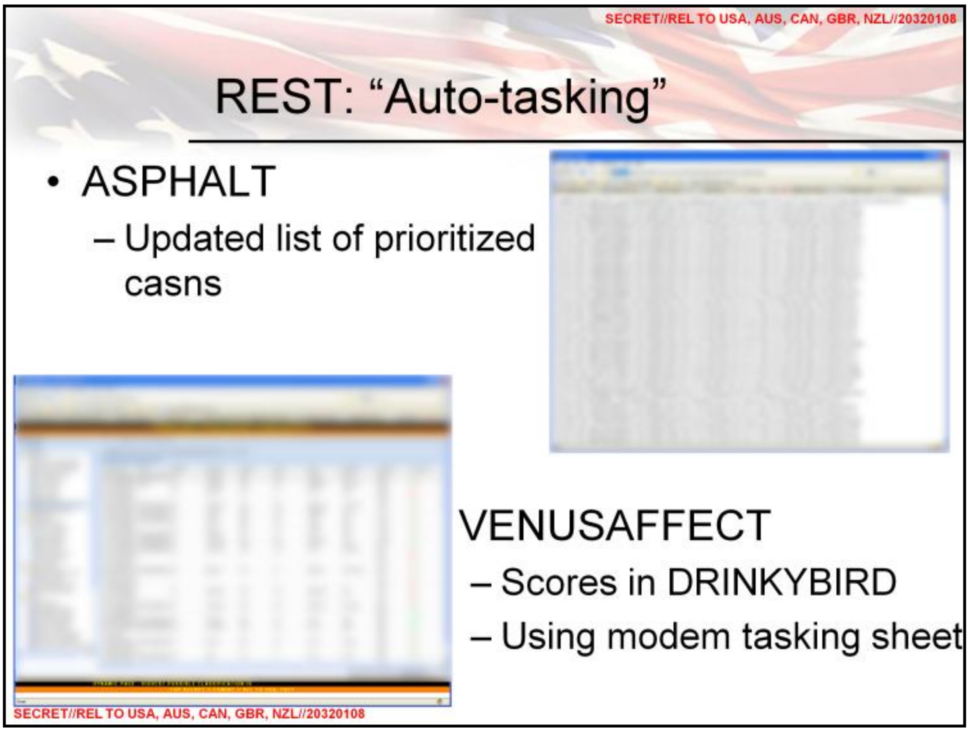
Focus Areas: Custom Views?


Home || All Questions || All CASNs || Survey CASNs || ASPHALT CASNs || Custom SQL Queries
Show 50 entries
Refresh

id	name	notes	active_score	first_run
2	geo	focus on geographical area	885195	2011-02-23
3	target	focus on target network or bad actor (via alert or dictionary hit)	528017	2011-01-19
5	other	focus on signal parameters, resource availability, casn type, etc	33050	2011-03-22
1	technology	focus on application or protocol	0	2011-03-30
4	compound	questions with multiple focus areas	0	2011-03-30

geo

question	topic	active score	weight	first contributed	last contributed
17	Libya	420000	1000	2011-02-23	2011-05-02
13	Egypt	187000	1000	2011-01-31	2011-05-02
25	Jordan	100000	1000	2011-03-17	2011-05-02
26	Syria	67000	1000	2011-03-21	2011-05-02
33	Syria GLOBETROTTER	42301	1000	2011-04-05	2011-05-02
6	Afghanistan	35900	50	2010-12-29	2011-05-02
32	Libya GLOBETROTTER	12661	100	2011-04-04	2011-05-02
24	Yemen	7000	1000	2011-03-17	2011-05-02
20	Qatar	6000	100	2011-03-03	2011-05-02
18	Bahrain	5100	100	2011-03-03	2011-05-02
34	Yemen GLOBETROTTER	1433	100	2011-04-05	2011-05-02
19	Oman	600	100	2011-03-03	2011-05-02
22	Algeria	100	100	2011-03-03	2011-05-02
21	Morocco	100	100	2011-03-03	2011-05-02
30	Libya Facebook	0	0	2011-03-30	2011-04-01
29	Libya Twitter	0	0	2011-03-30	2011-04-01
31	Libya TOR	0	0	2011-03-30	2011-04-01
9	Ivory Coast	null	200	2010-01-05	2011-05-02



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

REST: “Auto-tasking”

- ASPHALT
  - Updated list of prioritized casns

VENUSAFFECT
- Scores in DRINKYBIRD
- Using modem tasking sheet

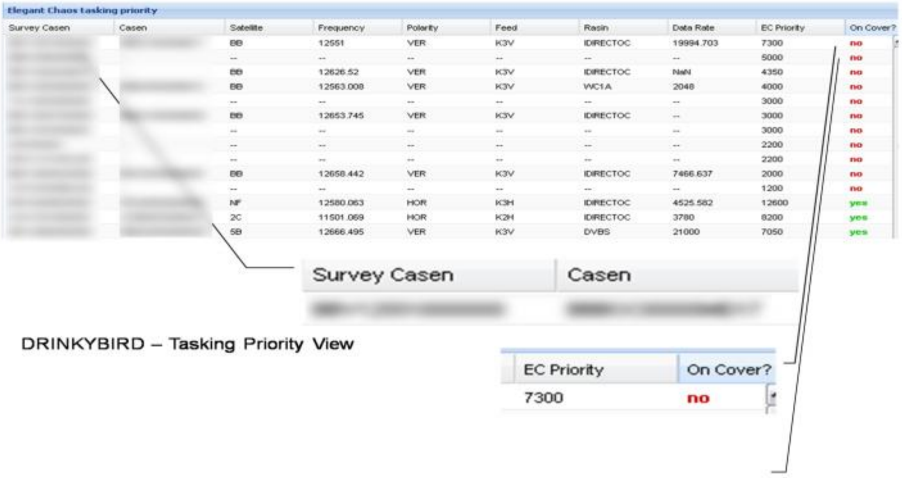
SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Interface to ASPHALT is easy with the developers on site !! – CSV file with required case notations FTP’d

Interface kludge into DRINKYBIRD – In-House network and tasking management GUI

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

DRINKYBIRD



Elegant Chaos tasking priority

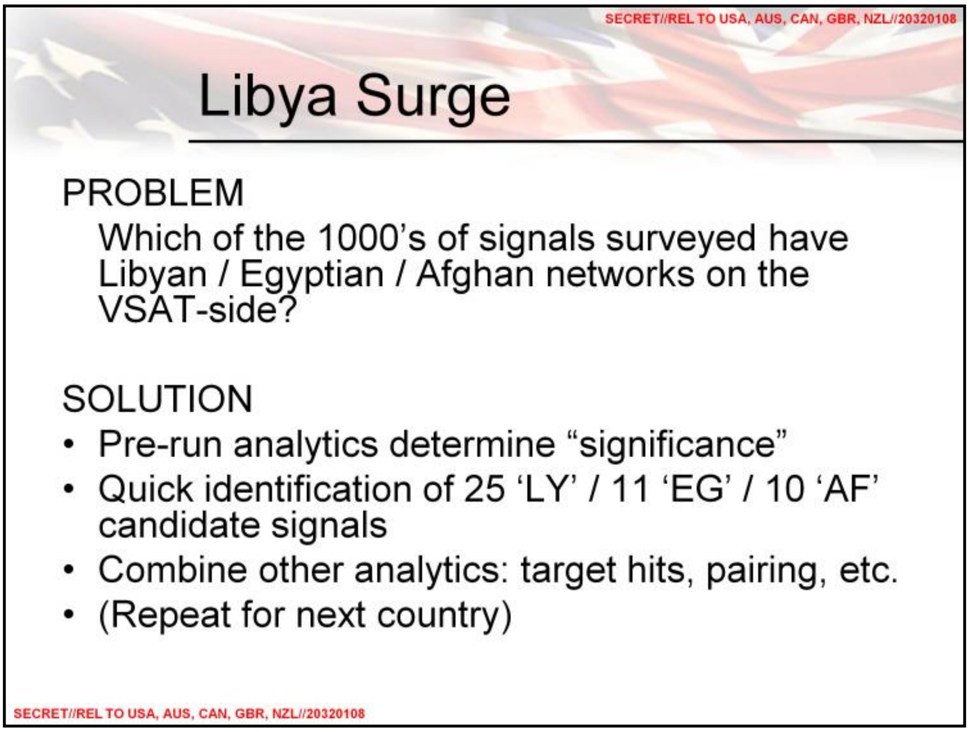
Survey Casen	Casen	Satellite	Frequency	Polarity	Feed	Rasin	Data Rate	EC Priority	On Cover?
[redacted]	[redacted]	BB	12551	VER	K3V	IDIRECTOC	19994.703	7300	no
[redacted]		--	--	--	--	--	--	5000	no
[redacted]		BB	12626.52	VER	K3V	IDIRECTOC	NaN	4350	no
[redacted]	[redacted]	BB	12563.008	VER	K3V	WC1A	2048	4000	no
[redacted]		--	--	--	--	--	--	3000	no
[redacted]	[redacted]	BB	12653.745	VER	K3V	IDIRECTOC	--	3000	no
[redacted]		--	--	--	--	--	--	3000	no
[redacted]		--	--	--	--	--	--	2200	no
[redacted]		--	--	--	--	--	--	2200	no
[redacted]	[redacted]	BB	12658.442	VER	K3V	IDIRECTOC	7466.637	2000	no
[redacted]		--	--	--	--	--	--	1200	no
[redacted]	[redacted]	NF	12580.063	HOR	K3H	IDIRECTOC	4525.582	12600	yes
[redacted]	[redacted]	2C	11501.069	HOR	K2H	IDIRECTOC	3780	8200	yes
[redacted]	[redacted]	5B	12666.495	VER	K3V	DVBS	21000	7050	yes

Survey Casen	Casen
[redacted]	[redacted]

DRINKYBIRD – Tasking Priority View

EC Priority	On Cover?
7300	no

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



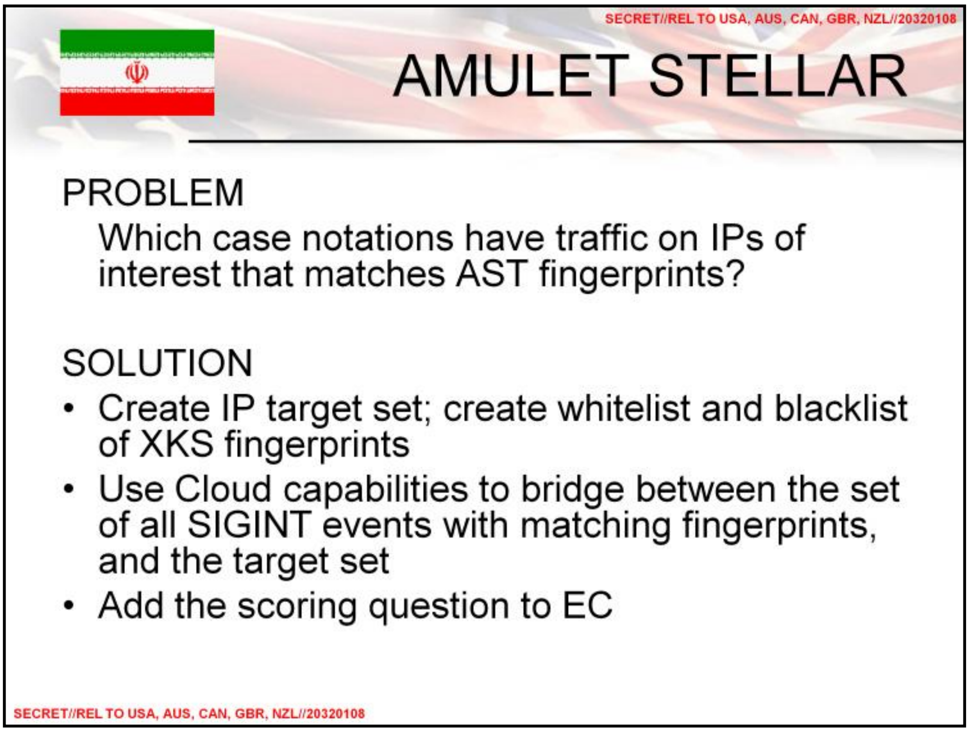
Libya Surge

PROBLEM

Which of the 1000's of signals surveyed have Libyan / Egyptian / Afghan networks on the VSAT-side?

SOLUTION

- Pre-run analytics determine "significance"
- Quick identification of 25 'LY' / 11 'EG' / 10 'AF' candidate signals
- Combine other analytics: target hits, pairing, etc.
- (Repeat for next country)



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

AMULET STELLAR

PROBLEM

Which case notations have traffic on IPs of interest that matches AST fingerprints?

SOLUTION

- Create IP target set; create whitelist and blacklist of XKS fingerprints
- Use Cloud capabilities to bridge between the set of all SIGINT events with matching fingerprints, and the target set
- Add the scoring question to EC

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

•Correlated IRC Botnet Activity to ASR Intrusion set (IRGC-QF Ramazan Corps Headquarters.)

•Discovered New Victims in Iraq and Iran

  •Multiple targets associated with S2E tasked selectors

•Discovered New Infrastructure

  •Engaged TAO for Vulnerability Assessment Evaluation

•Discovered potential C2, update and exfiltration nodes

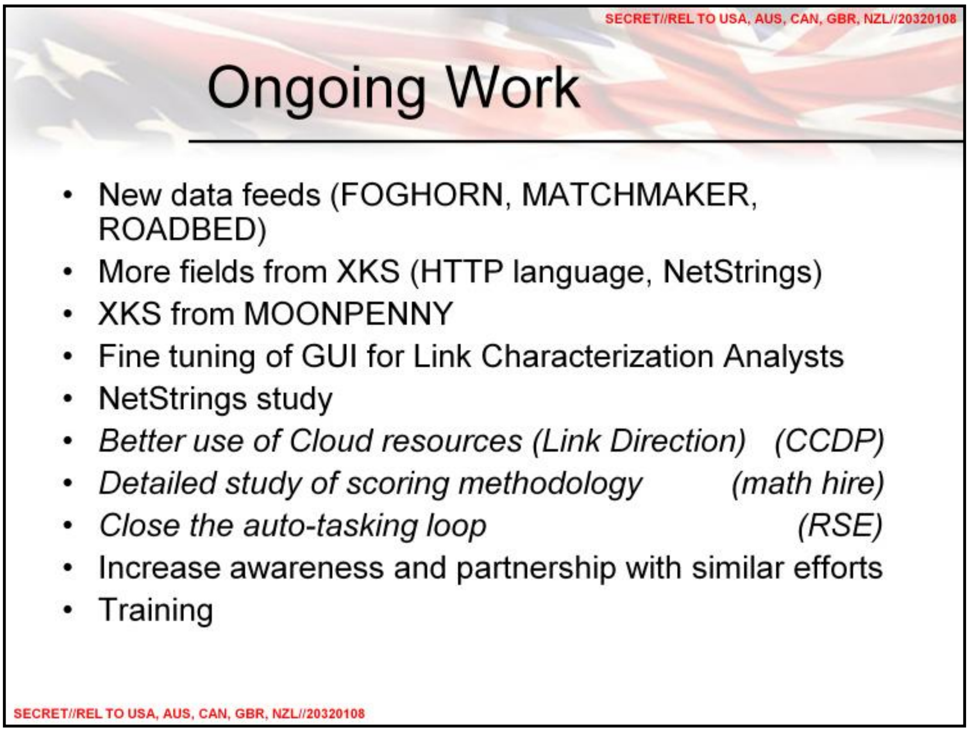
•Evaluating 4th Party Collection Opportunities

•Tipped: SSG, S2E, NTOC-G, TAO CCNE, documented in CROSSBONES.

•No specific fingerprints highlight this as ASR activity

  •Develop new “Infrastructure Agnostic” ASR fingerprints

•Use AES keys for decrypt and potential 4th party collection opportunity

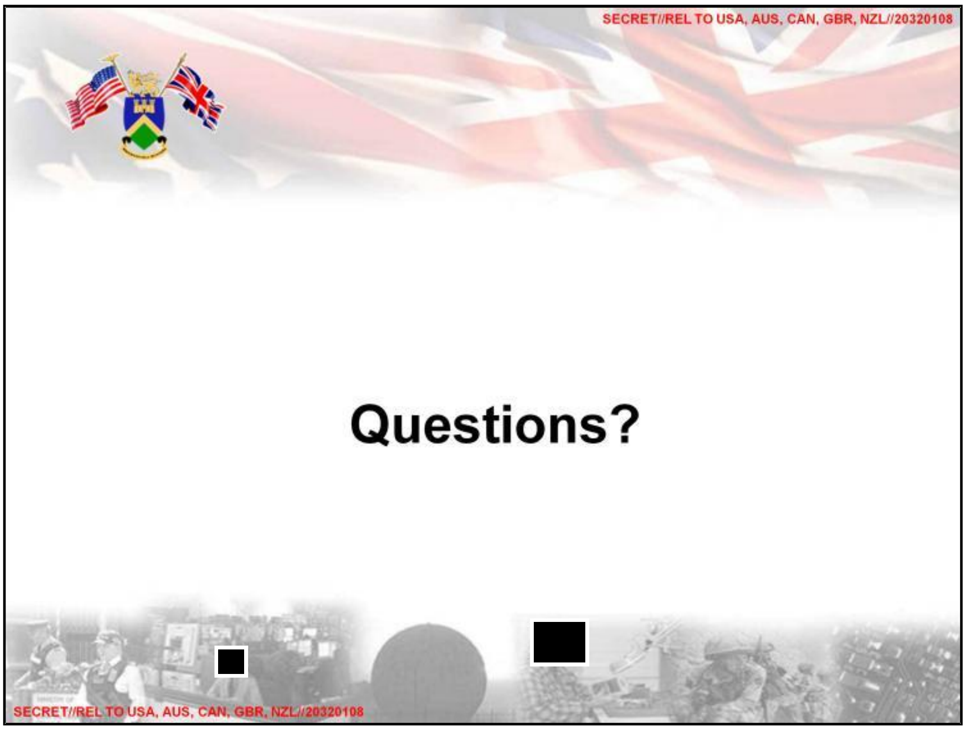


SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Ongoing Work

- New data feeds (FOGHORN, MATCHMAKER, ROADBED)
- More fields from XKS (HTTP language, NetStrings)
- XKS from MOONPENNY
- Fine tuning of GUI for Link Characterization Analysts
- NetStrings study
- *Better use of Cloud resources (Link Direction) (CCDP)*
- *Detailed study of scoring methodology (math hire)*
- *Close the auto-tasking loop (RSE)*
- Increase awareness and partnership with similar efforts
- Training

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108



SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Questions?

[redacted]

[redacted]

SECRET//REL TO USA, AUS, CAN, GBR, NZL//20320108

Is the enterprise considering SLR generation?