Synergising Network Analysis Tradecraft

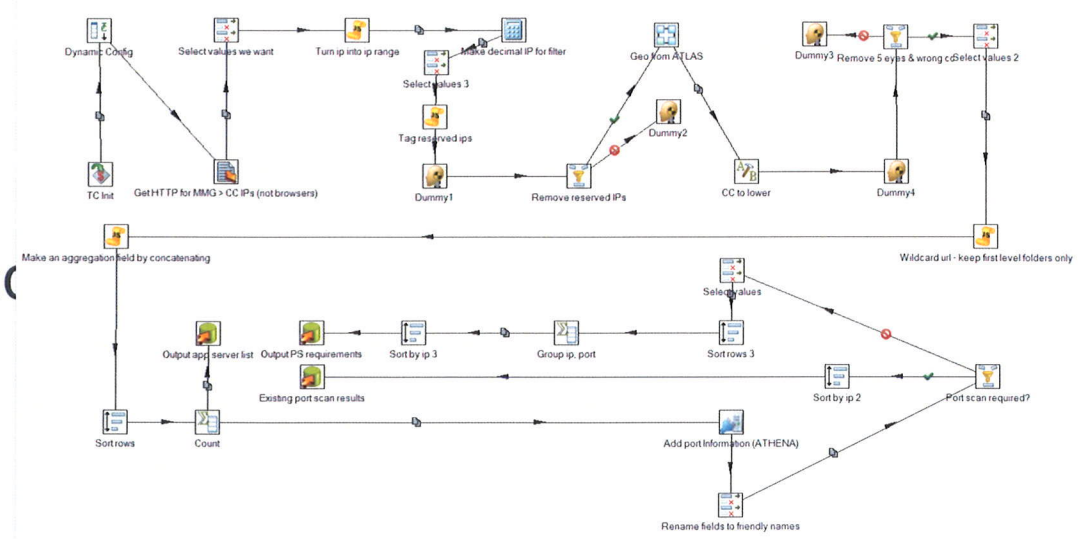
Network Tradecraft Advancement Team (NTAT)

DSD GCHQ GCSB NSA

Overview

* What is the NTAT?

* 2011 – 2012 work and accomplishments



Tradecraft?

Tradecraft

- "The development of methods, techniques, algorithms and processes in order to generate Intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques. **Industrial-Scale Tradecraft** involves data on a large scale."

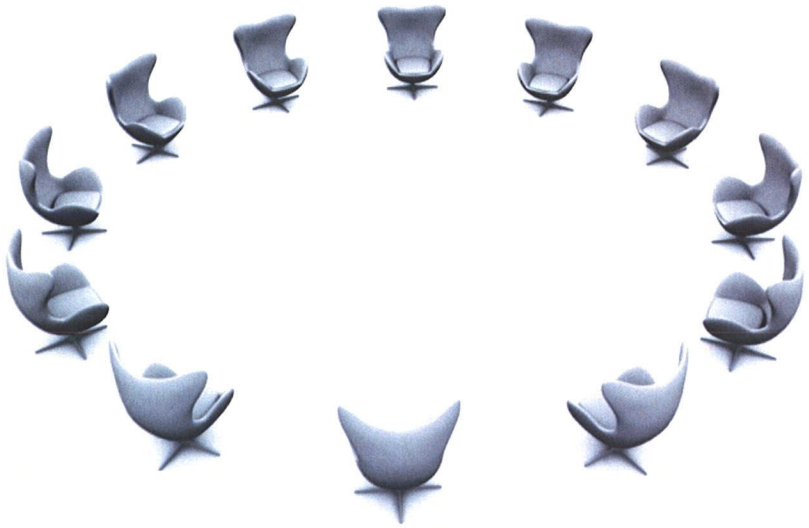
Network Tradecraft

- Usable knowledge about how to acquire intelligence FROM the network

The NTAT

* Create **repeatable**, **sustainable** & **shareable** tradecraft to enable network analysis

* Facilitate knowledge collaboration and interchange across the 5-Eyes SIGDEV community



The Process

Stage 1 = Fact Finding

Stage 2 = Define Focus (based on Fact Finding)

Stage 3 = Develop Tradecraft

Stage 4 = Document Tradecraft

Stage 5 = Test Documented Tradecraft and Refine

Network Convergence Tradecraft

* Technological convergence – where voice and data services interact with each other on a single device

* Tradecraft to enable the targeting of handsets in telephony space and CNE exploitation in IP space

* Improved algorithms for mobile gateway identification and implementation of these algorithms

DSD Workshop November 2011

* 2 weeks
  * CSE, DSD, GCHQ
  * Virtually, via chat room, NSA & GCSB
* Focus on data, techniques & analytic outcomes

https://wiki.dsd/twiki/[redacted]

DSD Workshop Outcomes

Technique developed to identify wide variety of potential converged data, unique for specific country or mobile network operator

- Ø ***potentially lead to convergence correlation dataset to help profile targets on-line activity***

Documentation of techniques to identify specific components of raw HTTP activity that alludes to the browsing, downloading and installation of smartphone applications

- Ø ***identified the presence of application servers for mobile network operators and geographical areas***

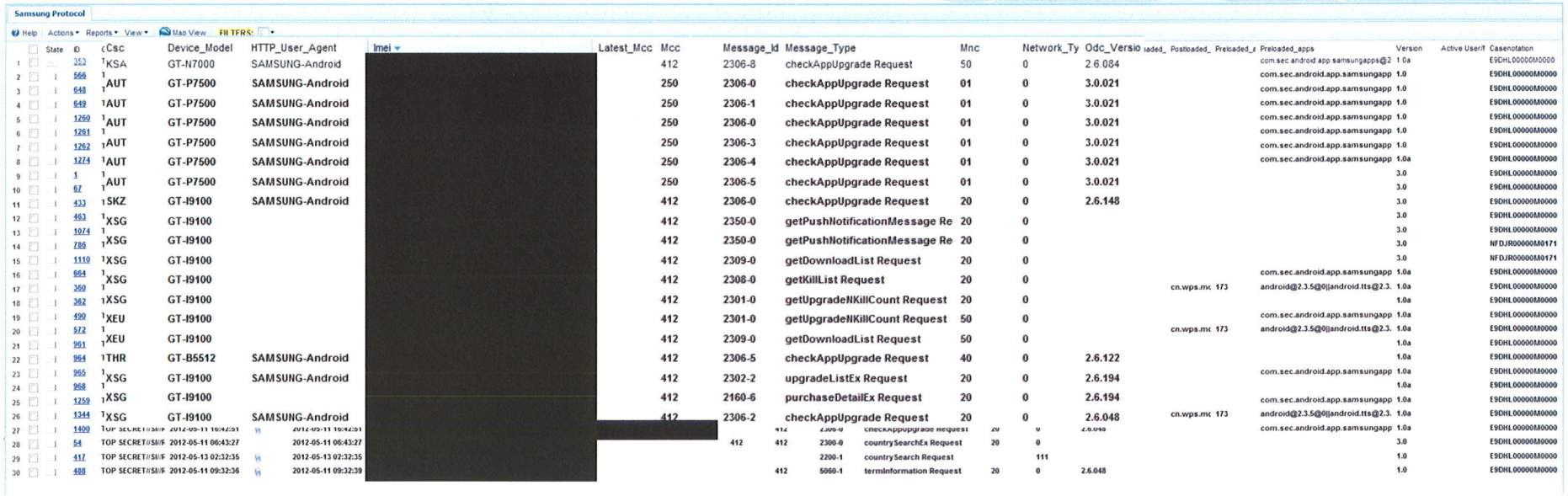
DSD implementation of mobile gateway identification analytic based on FRETTING YETI

- Ø ***three agencies now running the same analytic provides a richer dataset of mobile gateways***

CRAFTY SHACK trial

- Ø ***NTAT now using CRAFTY SHACK for tradecraft documentation***

XKS Microplugin: Samsung Protocol



Samsung Protocol

Help | Actions | Reports | View | Map View | FILTERS:

	State	ID	Csc	Device_Model	HTTP_User_Agent	Imei	Latest_Mcc	Mcc	Message_Id	Message_Type	Mnc	Network_Ty	Odc_Versio	aded_	Postloaded_	Preloaded_a	Preloaded_apps	Version	Active User/F	Casenotation
1		353	KSA	GT-N7000	SAMSUNG-Android	[redacted]		412	2306-8	checkAppUpgrade Request	50	0	2.6.084				com.sec.android.app.samsungapps@2	1.0a		E9DHL00000M0000
2		566	AUT	GT-P7500	SAMSUNG-Android			250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
3		648	AUT	GT-P7500	SAMSUNG-Android			250	2306-1	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
4		649	AUT	GT-P7500	SAMSUNG-Android			250	2306-0	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
5		1260	AUT	GT-P7500	SAMSUNG-Android			250	2306-3	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
6		1261	AUT	GT-P7500	SAMSUNG-Android			250	2306-4	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
7		1262	AUT	GT-P7500	SAMSUNG-Android			250	2306-5	checkAppUpgrade Request	01	0	3.0.021				com.sec.android.app.samsungapp	1.0		E9DHL00000M0000
8		1274	AUT	GT-P7500	SAMSUNG-Android			412	2306-0	checkAppUpgrade Request	20	0	2.6.148					3.0		E9DHL00000M0000
9		1	AUT	GT-P7500	SAMSUNG-Android			412	2350-0	getPushNotificationMessage Re	20	0						3.0		E9DHL00000M0000
10		67	AUT	GT-P7500	SAMSUNG-Android			412	2350-0	getPushNotificationMessage Re	20	0						3.0		NFDJR00000M0171
11		433	SKZ	GT-I9100	SAMSUNG-Android			412	2309-0	getDownloadList Request	20	0						3.0		NFDJR00000M0171
12		463	XSG	GT-I9100				412	2308-0	getKillList Request	20	0					com.sec.android.app.samsungapp	1.0a		E9DHL00000M0000
13		1074	XSG	GT-I9100				412	2301-0	getUpgradeNKillCount Request	20	0			cn.wps.mc	173	android@2.3.5@0|android.tts@2.3.	1.0a		E9DHL00000M0000
14		786	XSG	GT-I9100				412	2301-0	getUpgradeNKillCount Request	50	0					com.sec.android.app.samsungapp	1.0a		E9DHL00000M0000
15		1110	XSG	GT-I9100				412	2309-0	getDownloadList Request	50	0			cn.wps.mc	173	android@2.3.5@0|android.tts@2.3.	1.0a		E9DHL00000M0000
16		664	XSG	GT-I9100				412	2306-5	checkAppUpgrade Request	40	0	2.6.122					1.0a		E9DHL00000M0000
17		360	XEU	GT-I9100				412	2302-2	upgradeListEx Request	20	0	2.6.194				com.sec.android.app.samsungapp	1.0a		E9DHL00000M0000
18		362	XSG	GT-I9100				412	2160-6	purchaseDetailEx Request	20	0	2.6.194					1.0a		E9DHL00000M0000
19		490	XEU	GT-I9100				412	2306-2	checkAppUpgrade Request	20	0	2.6.048				com.sec.android.app.samsungapp	1.0a		E9DHL00000M0000
20		572	XEU	GT-I9100				412	2306-0	checkAppUpgrade Request	20	0	2.6.048		cn.wps.mc	173	android@2.3.5@0|android.tts@2.3.	1.0a		E9DHL00000M0000
21		961	XEU	GT-I9100				412	2300-0	countrySearchEx Request	20	0					com.sec.android.app.samsungapp	1.0a		E9DHL00000M0000
22		964	THR	GT-B5512	SAMSUNG-Android			412	2200-1	countrySearch Request		111						1.0		E9DHL00000M0000
23		965	XSG	GT-I9100	SAMSUNG-Android			412	5060-1	terminformation Request	20	0	2.6.048					1.0		E9DHL00000M0000
24		968	XSG	GT-I9100																
25		1259	XSG	GT-I9100																
26		1344	XSG	GT-I9100	SAMSUNG-Android															
27		1400	TOP SECRET//SI/F	2012-05-11 16:47:51		2012-05-11 16:47:51														
28		54	TOP SECRET//SI/F	2012-05-11 06:43:27		2012-05-11 06:43:27														
29		417	TOP SECRET//SI/F	2012-05-13 02:32:35		2012-05-13 02:32:35														
30		488	TOP SECRET//SI/F	2012-05-11 09:32:36		2012-05-11 09:32:39														

CSE Workshop February 2012

* 2 weeks
  * CSE, DSD, GCHQ, GCSB, NSA – everyone wanted to experience a Canadian winter!
  * Build on the work started at DSD

Winter Nirvana

The Reality!

CSE Workshop Outcomes

Refinement of XKS fingerprints to identify mobile bearers, Samsung and Android Marketplace servers

- ***17 XKS fingerprints deployed***

Documentation of analytics in CRAFTY SHACK

- ***These analytics are now being implemented across the 5 Eyes***

Proving the tradecraft actually works!

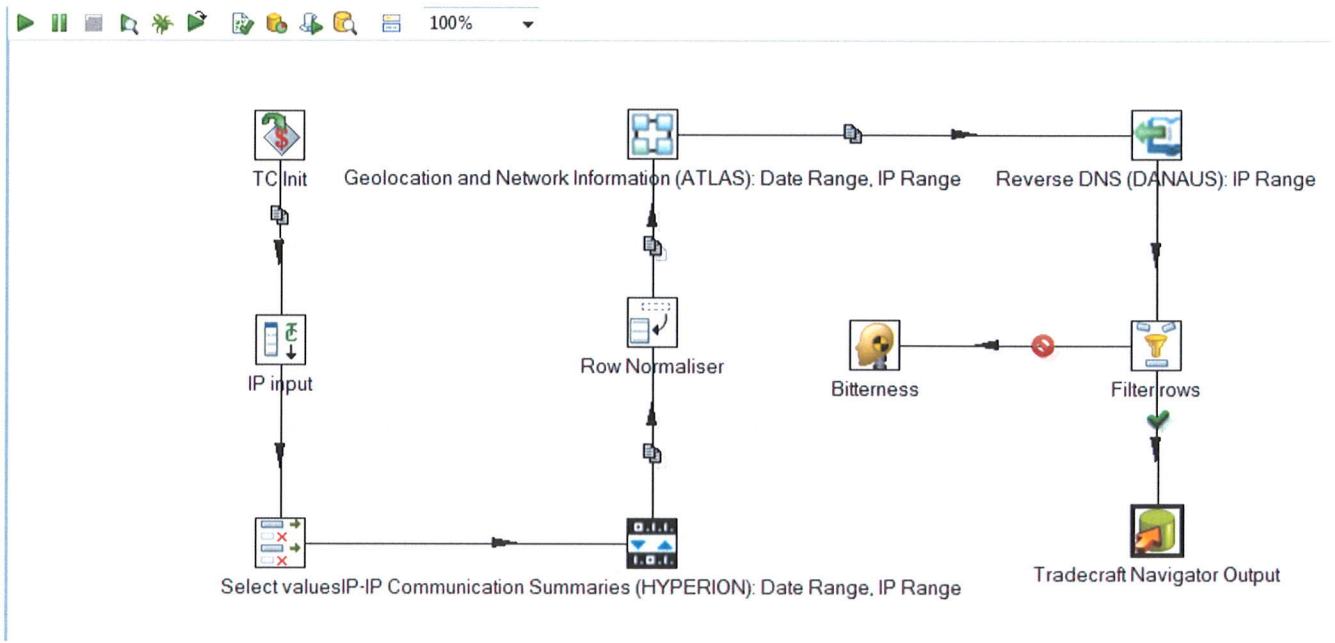
- ***Scenario to test the tradecraft and analytics – Op IRRITANT HORN***

Op IRRITANT HORN

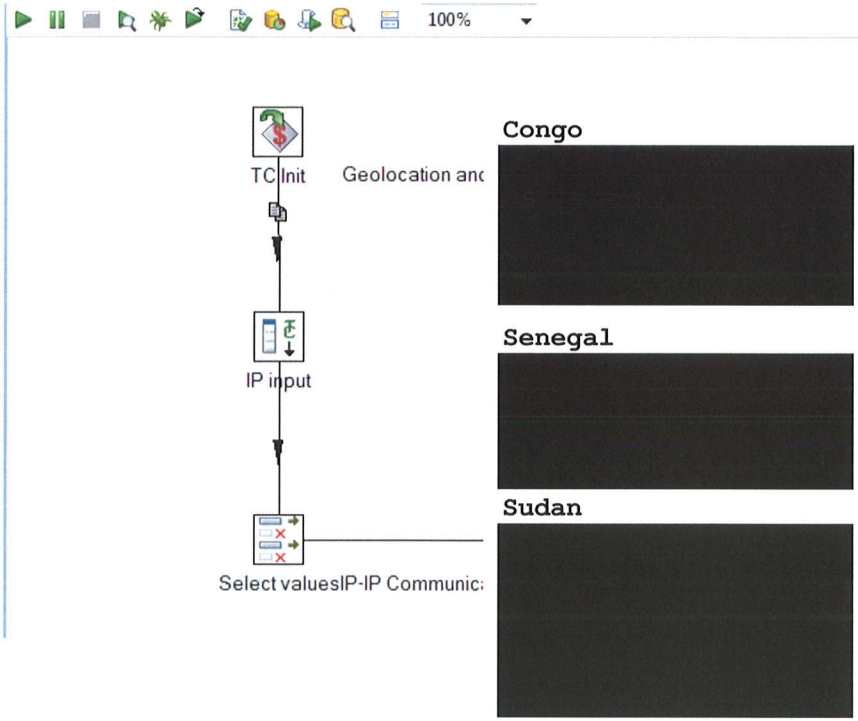
Op IRRITANT HORN
Does the tradecraft work?

* Another Arab Spring (only this time, different countries)
* Goal: identify aggregation points for the mobile networks in the countries of interest using the tradecraft developed during the workshops
* Did it work? YES -> the team was able to identify connections from the countries to application and vendor servers in non 5-Eyes countries
* So what? We found some servers….
  - Ø Potential MiTM
  - Ø Effects
  - Ø Harvesting data at rest
  - Ø Harvesting data in transit

Finding mobile application & vendor update servers



Finding mobile application & vendor update servers



france	android-market.l.google.com
france	android-market.l.google.com
france	android-market.l.google.com
france	android-market.l.google.com
france	android-market.l.google.com
cuba	store.cubava.cu
cuba	store.cubava.cu
senegal	srv_applis.sar.sn
morocco	boungeontelephone.com
switzerland	download-force.com
bahamas	supportapple.com
cuba	store.cubava.cu
netherlands	mobile.ero-advertising.com
russia	lady.marketgid.info

Crafty Shack

Change view [redacted]@cse-cst.gc.ca

Search this wiki | Go | Search

Browse ▾ Search ▾ Create ▾ Help ▾ MediaWiki ▾

Identify Servers communicating with a Mobile network

Page Discussion History Edit

SECRET

Identify Servers communicating with a Mobile network

5 EYES | CSEC | DSD | GCHQ | GCSB | NSA | Factbox

Metadata

What does the tradecraft achieve?

- This tradecraft will provide a list of servers that have been seen communicating with a mobile network.

In what situations would this tradecraft be most useful?

- To identify mobile application servers for a specific network
- To identify any server that may be useful for collection purposes

Describe any problems, caveats or things to watch out for

- The list of servers returned depends on the the IP range and collection sources utilized. Success of this tradecraft may require additional research to identify other IP ranges or requesting other agencies to check their collection to identify different servers.

Links that can help you to implement this tradecraft

Created by: [redacted]
Agency: NSA
Email Address: [redacted]

Difficulty: ☆ ☆ ☆

Acceptance state: Limited

Input(s): Ontology:Network block, Ontology:Ip address **Output(s):** Ontology:Ip address, Ontology:ASN, Ontology:Network block, Ontology:Hostname, Ontology:User Agent String, Ontology:Geographic selector

Invokes Tradecraft:
- Find public IP space used by Mobile Devices and Related Servers on the Internet
- Finding Mobile Internet Gateways

Input(s): Ontology:Network block, Ontology:Ip address **Output(s):** Ontology:Ip address, Ontology:ASN, Ontology:Network block, Ontology:Hostname, Ontology:User Agent String, Ontology:Geographic selector

Invokes Tradecraft:
- Find public IP space used by Mobile Devices and Related Servers on the Internet
- Finding Mobile Internet Gateways

Alternatives:
- **Identify Servers communicating with a Mobile network**

5 EYES Tradecraft Steps (document underlying analytic, do not include tools) [edit]

The IP ranges utilized for the initial implementation of this tradecraft were the Inter PLMN Backbone IP ranges obtained from IR21 documents. For other methods of identifying mobile IP blocks, see the invoked tradecraft listed above.

Step 1) Take IP ranges or individual addresses identified as being related to mobile network communications.
Step 2) Obtain geolocation information and network ownership information for each IP address. This should include: Network Owner name, Carrier name, ASN, Continent, Country, Region, City, Lat/Long, and any other related details that your system can obtain.
Step 3) Obtain Internet communication events related to the IP addresses. These events should minimally include: source information, To IP, From IP, TCP Direction, and HTTP User-Agent
Step 4) Sort the results and dedup them. This step depends on your collection sources.
Step 5) Filter out server communications that have user-agents that aren't useful. Further analysis is needed to identify the non-useful user-agents (cheat sheet needed). Ex friendly-scanner
Step 6) Check the TCP Direction field:
- If Server to Client, grab the From IP information
- If Client to Server, grab the To IP information
- If Server to Server, grab both the To and From IP information
- If Unknown, capture in an error log

Step 7) Sort and dedup again based on Server IP information. TCP Direction info is no longer needed.
Step 8) Obtain geolocation information and network ownership information for each Server IP. This is done for the servers that were not in the original IP Blocks.
Step 9) Remove any servers that are not useful. This may include 5-Eyes servers.
Step 10) Output:
- List of Servers
- List of related User Agents
- List of related hostnames

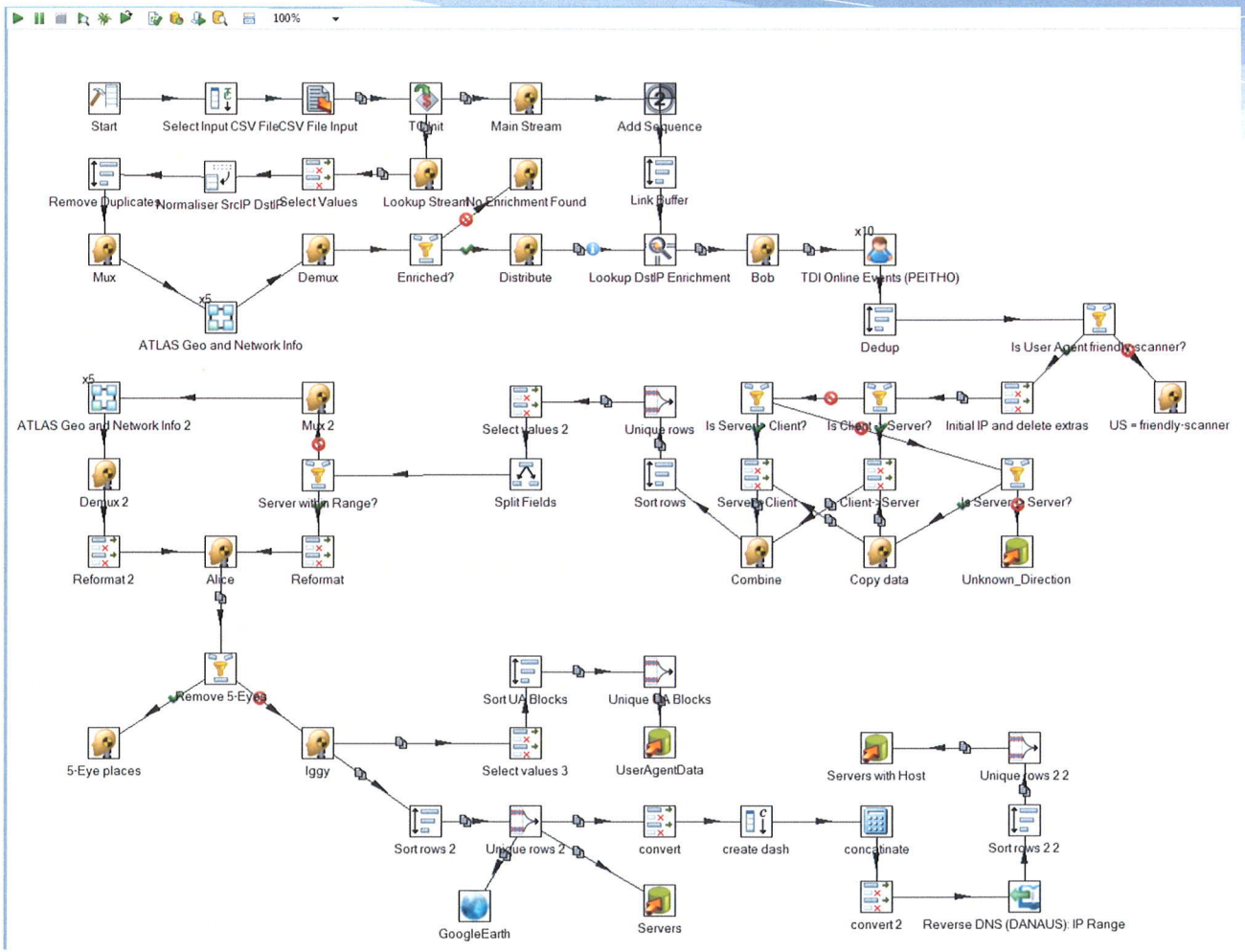
Comments (2) | Show comments Average article quality based on 1 rating(s)

Last updated: 24/2/2012 by [redacted]

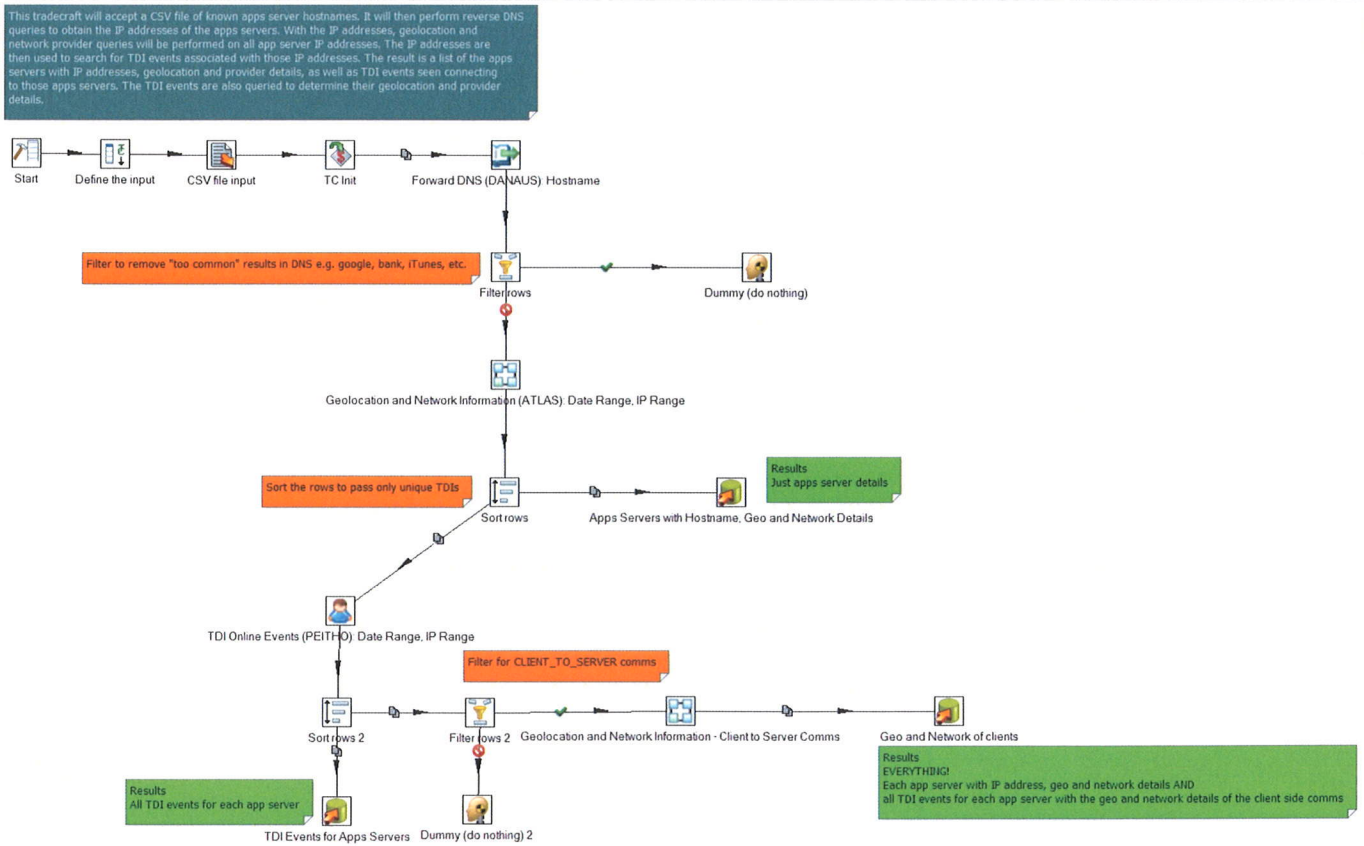
Category: Tradecraft

CRAFTY SHACK - *"It's not tradecraft until it's documented! - [redacted] CSEC"* [edit]

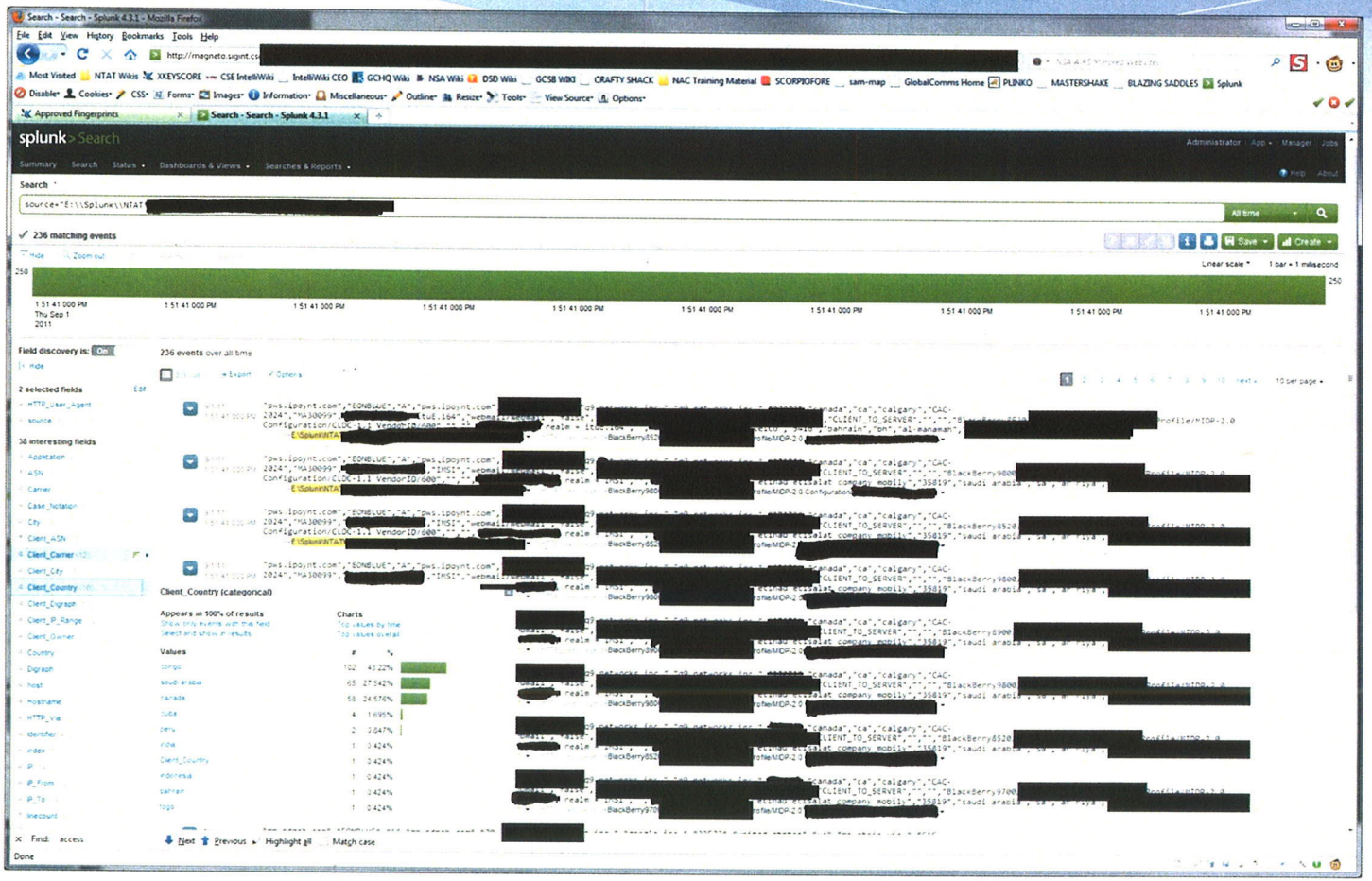
Identifying servers communicating with an MNO



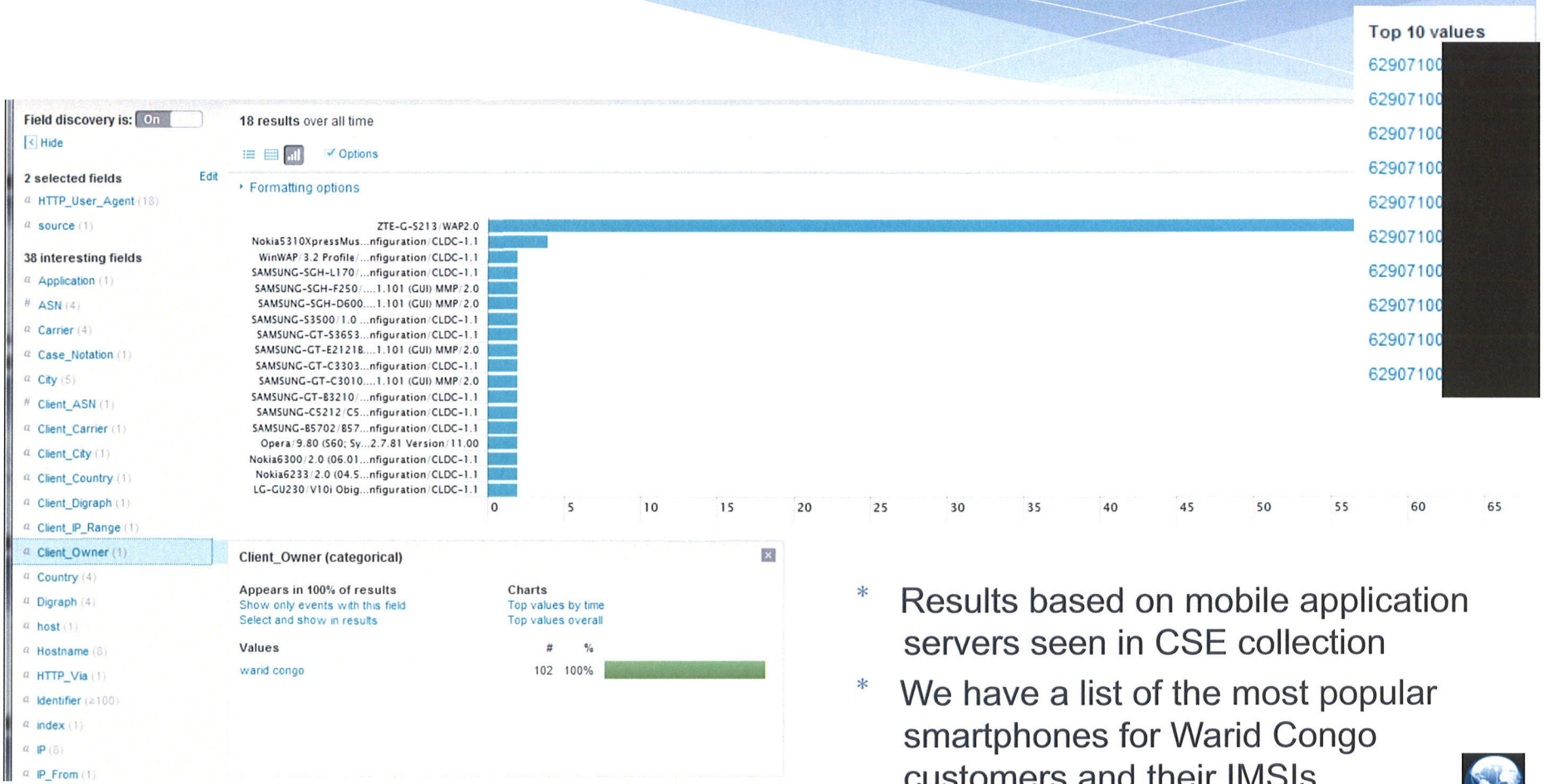
Profiling mobile application servers



Profiling mobile application servers



Profiling mobile application servers



* Results based on mobile application servers seen in CSE collection
* We have a list of the most popular smartphones for Warid Congo customers and their IMSIs

Success Stories

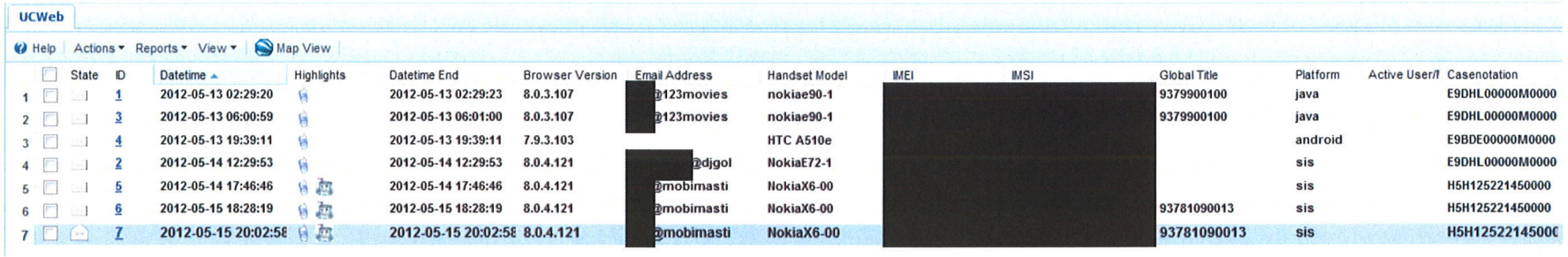
* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop
  * Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics

UCWeb

* Led to discovery of active comms channel from [redacted]

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a ***Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection****. The covert channel originates from users who use UCBrowser (mobile phone compact web browser).* ***The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in*** *[redacted] Initial investigation has determined that perhaps malware can be associated when the covert channel is established. [redacted] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence*

UCWeb – XKS Microplugin



UCWeb

Help | Actions | Reports | View | Map View

	State	ID	Datetime	Highlights	Datetime End	Browser Version	Email Address	Handset Model	IMEI	IMSI	Global Title	Platform	Active User/I	Casenotation
1		1	2012-05-13 02:29:20		2012-05-13 02:29:23	8.0.3.107	[redacted]@123movies	nokiae90-1	[redacted]		9379900100	java		E9DHL00000M0000
2		3	2012-05-13 06:00:59		2012-05-13 06:01:00	8.0.3.107	[redacted]@123movies	nokiae90-1			9379900100	java		E9DHL00000M0000
3		4	2012-05-13 19:39:11		2012-05-13 19:39:11	7.9.3.103		HTC A510e				android		E9BDE00000M0000
4		2	2012-05-14 12:29:53		2012-05-14 12:29:53	8.0.4.121	[redacted]@djgol	NokiaE72-1				sis		E9DHL00000M0000
5		5	2012-05-14 17:46:46		2012-05-14 17:46:46	8.0.4.121	[redacted]@mobimasti	NokiaX6-00				sis		H5H125221450000
6		6	2012-05-15 18:28:19		2012-05-15 18:28:19	8.0.4.121	[redacted]@mobimasti	NokiaX6-00			93781090013	sis		H5H125221450000
7		7	2012-05-15 20:02:58		2012-05-15 20:02:58	8.0.4.121	[redacted]@mobimasti	NokiaX6-00			93781090013	sis		H5H12522145000

Vision of Success

* Shared convergence database with numerous different sources, methods & tradecraft feeding into it
* Ultimately correlating telephony and Internet TDIs with some degree of confidence

Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)

DSD GCHQ GCSB NSA

Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)

Overview

* What is the NTAT?
* 2011 – 2012 work and accomplishments

TOP SECRET//SI

Tradecraft?

Tradecraft

- "The development of methods, techniques, algorithms and processes in order to generate Intelligence, and developing the ability to apply this knowledge either manually or through automation. Tradecraft is developed from experience, research, intuition and by the reapplication and redefinition of existing techniques. **Industrial-Scale Tradecraft** involves data on a large scale."

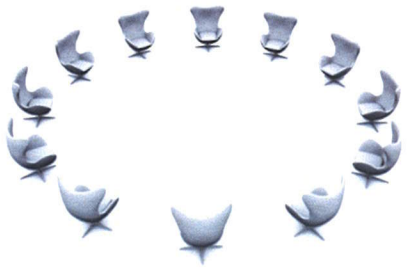
Network Tradecraft

- Usable knowledge about how to acquire intelligence FROM the network

TOP SECRET//SI

The NTAT

- Create **repeatable**, **sustainable** & **shareable** tradecraft to enable network analysis
- Facilitate knowledge collaboration and interchange across the 5-Eyes SIGDEV community



TOP SECRET//SI

The Process

Stage 1 = Fact Finding

Stage 2 = Define Focus (based on Fact Finding)

Stage 3 = Develop Tradecraft

Stage 4 = Document Tradecraft

Stage 5 = Test Documented Tradecraft and Refine

TOP SECRET//SI

Network Convergence Tradecraft

* Technological convergence – where voice and data services interact with each other on a single device
* Tradecraft to enable the targeting of handsets in telephony space and CNE exploitation in IP space
* Improved algorithms for mobile gateway identification and implementation of these algorithms

TOP SECRET//SI

DSD Workshop
November 2011

* 2 weeks
  * CSE, DSD, GCHQ
  * Virtually, via chat room, NSA & GCSB
* Focus on data, techniques & analytic outcomes

https://wiki.dsd/twiki/[redacted]

DSD Workshop Outcomes

Technique developed to identify wide variety of potential converged data, unique for specific country or mobile network operator

- ***potentially lead to convergence correlation dataset to help profile targets on-line activity***

Documentation of techniques to identify specific components of raw HTTP activity that alludes to the browsing, downloading and installation of smartphone applications

- ***identified the presence of application servers for mobile network operators and geographical areas***

DSD implementation of mobile gateway identification analytic based on FRETTING YETI

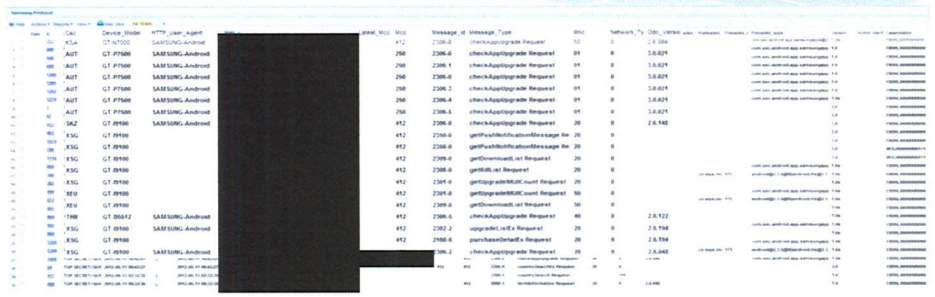
- ***three agencies now running the same analytic provides a richer dataset of mobile gateways***

CRAFTY SHACK trial

- ***NTAT now using CRAFTY SHACK for tradecraft documentation***

TOP SECRET//SI

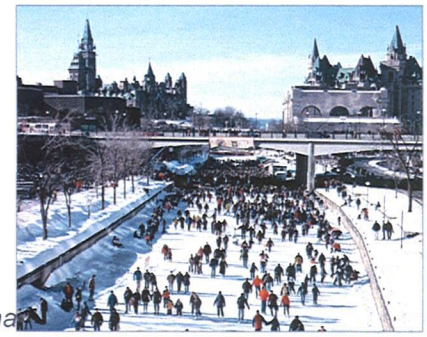
XKS Microplugin: Samsung Protocol



TOP SECRET//SI

CSE Workshop
February 2012

- 2 weeks
  - CSE, DSD, GCHQ, GCSB, NSA – everyone wanted to experience a Canadian winter!
  - Build on the work started at DSD



Winter Nirvana

The Reality!

CSE Workshop Outcomes

Refinement of XKS fingerprints to identify mobile bearers, Samsung and Android Marketplace servers

- ***17 XKS fingerprints deployed***

Documentation of analytics in CRAFTY SHACK

- ***These analytics are now being implemented across the 5 Eyes***

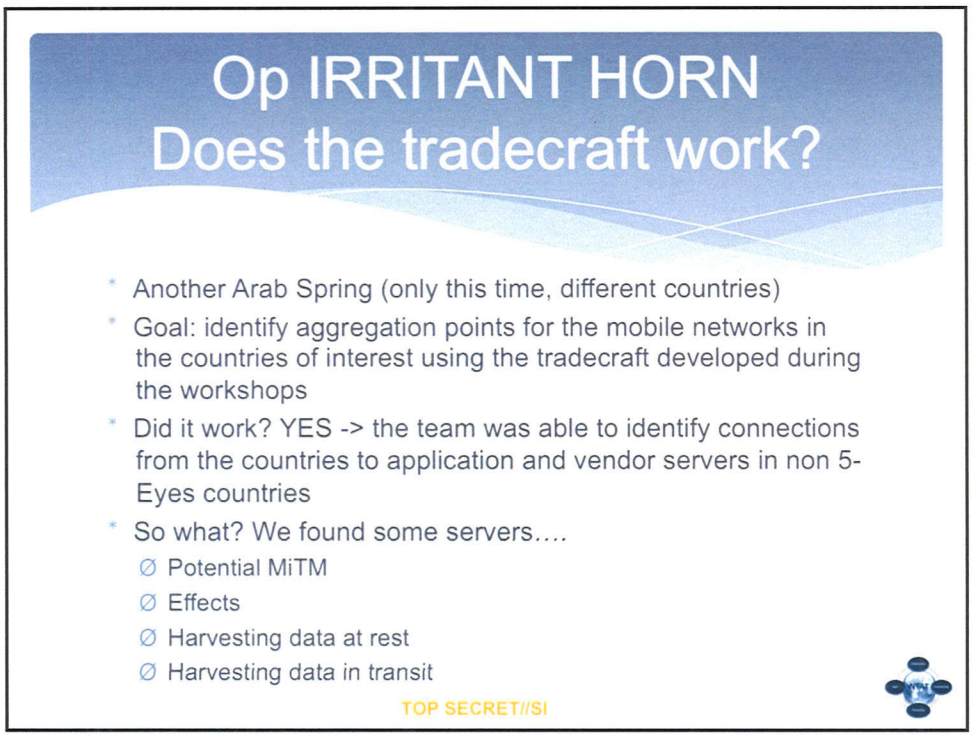
Proving the tradecraft actually works!

- ***Scenario to test the tradecraft and analytics – Op IRRITANT HORN***

TOP SECRET//SI

Op IRRITANT HORN

TOP SECRET//SI

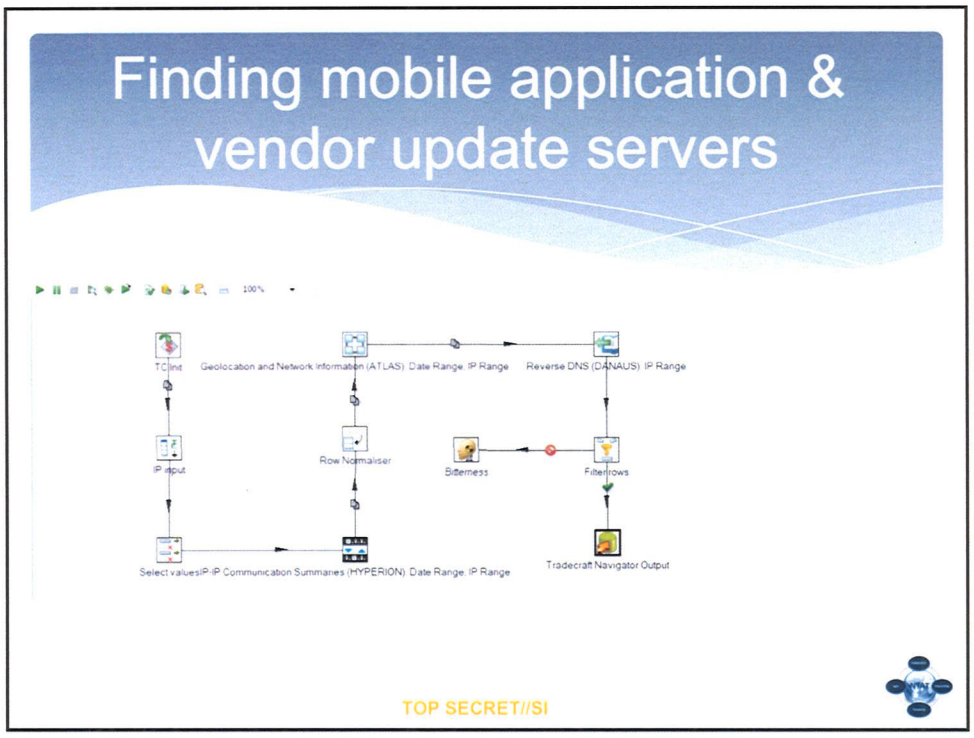


MiTM – exploit the application server and use it as a MiTM platform for handset exploitation

Effects – exploitation of the application servers could make it possible to provide selective misinformation to the targets handsets

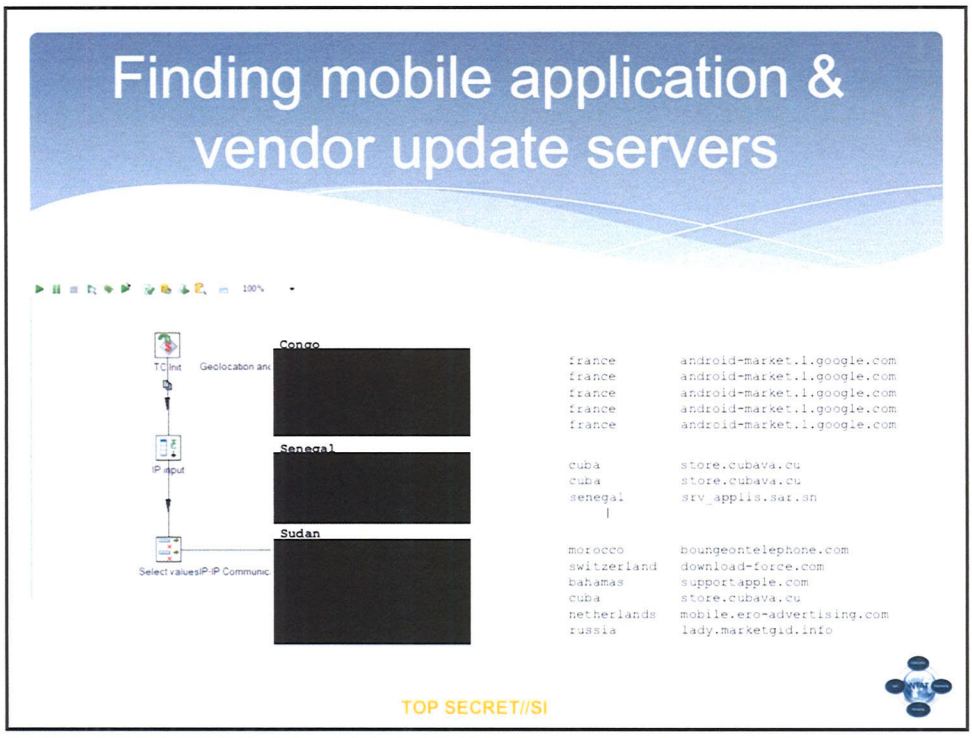
Harvesting data at rest – exploitation of the applications servers could provide access to a wealth of information at rest. The amount and usefulness of this information depends on the application in question

Harvesting data in transit – mobile applications servers often send and receive data that SIGINT agencies find useful (e.g. the Samsung protocol sending client and handset details to a server in Germany)



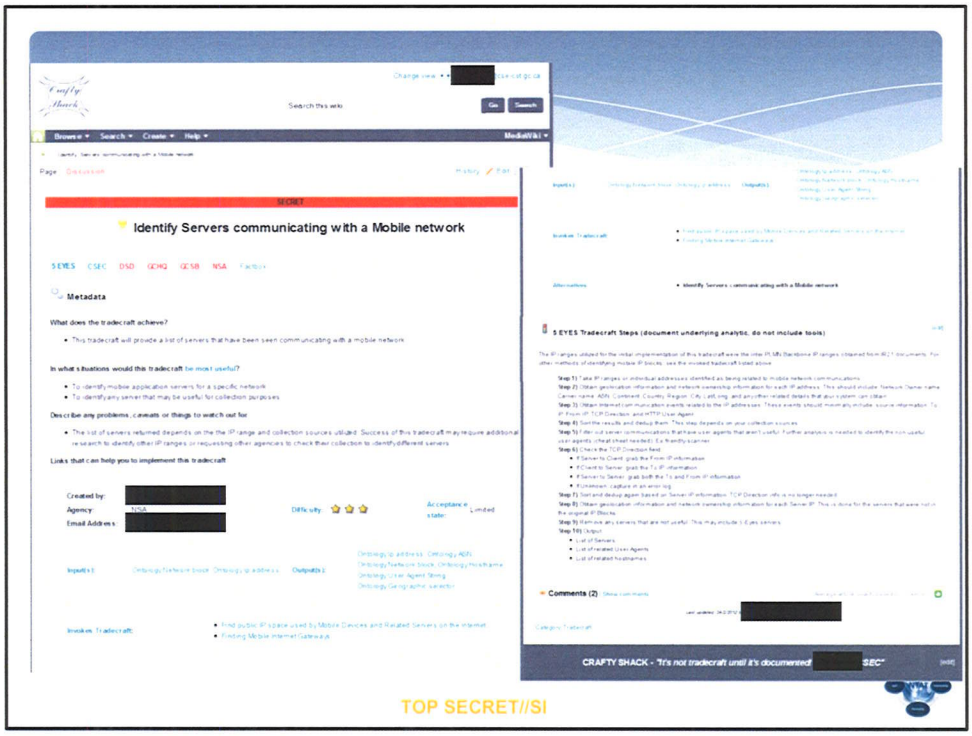
The results above are from a tradecraft to find servers of applications and vendor updaters servers from given countries, The rationale behind this is to identify servers that target within those countries might visit which could be exploited by CNE to push a phone implant capability.

The tradecraft relies upon 5 tuple data seen from the mobile gateways from target countries and to servers which have matching 'key words' in the hostname. The results above could then be scoped for CNE to see if they would be valid boxes to use an access platform.

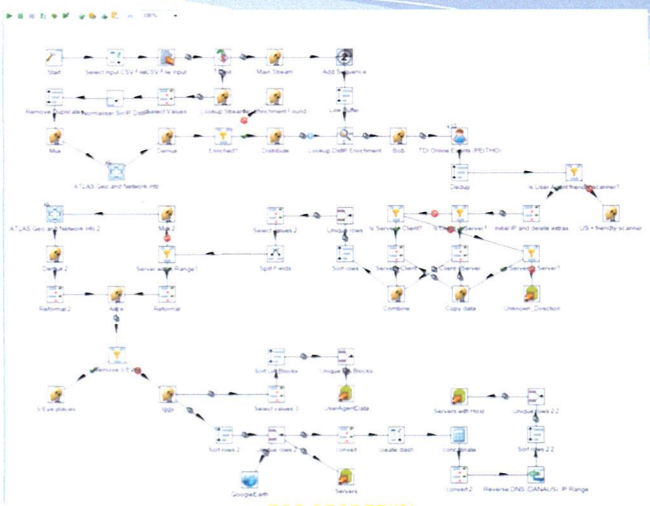


The results above are from a tradecraft to find servers of applications and vendor updaters servers from given countries, The rationale behind this is to identify servers that target within those countries might visit which could be exploited by CNE to push a phone implant capability.

The tradecraft relies upon 5 tuple data seen from the mobile gateways from target countries and to servers which have matching 'key words' in the hostname. The results above could then be scoped for CNE to see if they would be valid boxes to use an access platform.

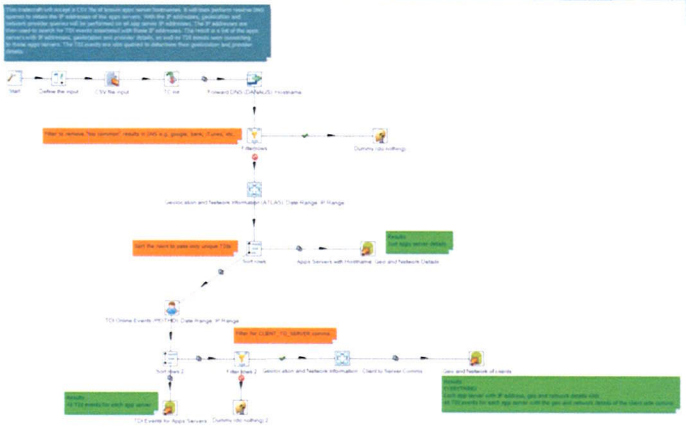

Identify Servers communicating with a Mobile network
SECRET
Metadata
What does the tradecraft achieve?
In what situations would this tradecraft be most useful?
Describe any problems, caveats or things to watch out for
Links that can help you to implement this tradecraft
Created by:
Agency:
Email Address:
Difficulty:
Acceptance state:
Inputs (1):
Outputs (1):
Invokes Tradecraft:
5 EYES Tradecraft Steps (document underlying analytic, do not include tools)
Comments (2)
CRAFTY SHACK - "It's not tradecraft until it's documented
SEC"
TOP SECRET//SI

Identifying servers communicating with an MNO



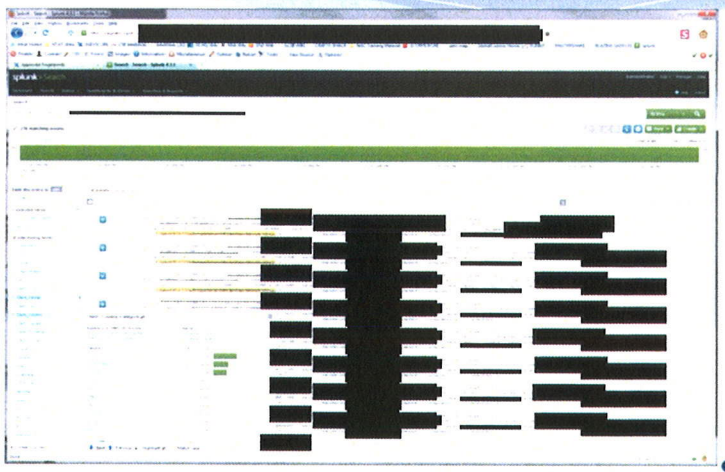
TOP SECRET//SI

Profiling mobile application servers



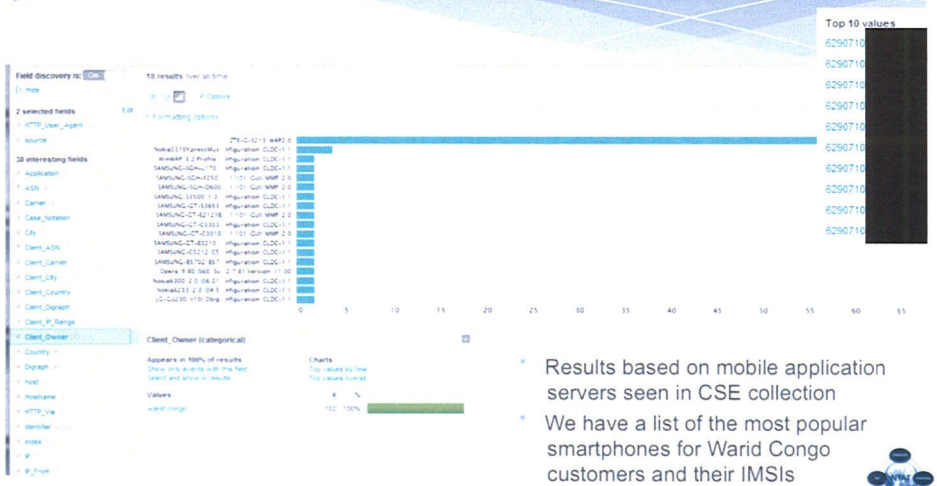
TOP SECRET//SI

Profiling mobile application servers



TOP SECRET//SI

Profiling mobile application servers



- Results based on mobile application servers seen in CSE collection
- We have a list of the most popular smartphones for Warid Congo customers and their IMSIs

TOP SECRET//SI

Success Stories

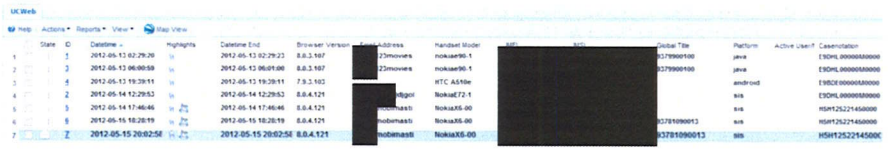
* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop
  * Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics

UCWeb

- Led to discovery of active comms channel from [redacted]

(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from [redacted] that is associated with the [redacted] as they are known within the [redacted] hierarchy area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a ***Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection****. The covert channel originates from users who use UCBrowser (mobile phone compact web browser).* ***The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in*** [redacted] *Initial investigation has determined that perhaps malware can be associated when the covert channel is established [redacted] covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence.*

UCWeb – XKS Microplugin



TOP SECRET//SI

Vision of Success

* Shared convergence database with numerous different sources, methods & tradecraft feeding into it
* Ultimately correlating telephony and Internet TDIs with some degree of confidence

TOP SECRET//SI

Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)