Broadcast/Internet Radio Exploitation and Analysis

[redacted]@gchq

6th November 2009

OPD-NAC

Distribution (via email)

GCHQ
[redacted] (TR)
[redacted] (GTE)
[redacted] (JTRIG)
[redacted] (CRFC)
[redacted] (FTCG)
[redacted] (CNE)

SIS
[redacted] (ST2)

BSS
[redacted] (C3T-4)

2nd Parties
[redacted] (NSA)

Report Summary

Author	[redacted]
Primary Customer	TR-CISA
SDTD Reference	N/A
Contributing Analysts	[redacted]
Key Terms	Broadcast, Icecast, Shoutcast, Peercast, Internet Radio
Soft Copy Location	T:_S\Sigint Development\GNE Restricted\NAC Reports
Relevant CMAPs	N/A
See Also	Strategic Framework Task 4134544, 72/09/R/001/C

Context

1.1 Internet Radio is a technology that allows audio streams, usually based on MP3 or AAC formats, to be broadcast over the Internet to clients in real-time.

Details

1.2 This report documents the results of an analysis into data derived from on-line broadcasting, or "Internet radio". This technology allows users to broadcast audio via the internet without the restrictions traditionally associated with broadcasting.

1.1 The technology covers protocols such as "Shoutcast", "Icecast" and "Peercast". Further details of the technology are summarised in report 4134544 [1]

1.2 The interception capability was delivered under Strategic Framework Task 4134544 by TR-CISA and was deployed at CPC in the PPF framework.

1.3 A sample of the derived SIGINT data was taken over 3-month period (August-October 2009). This sample represented 6.68 Million unique events from the accesses feeding the research system. These accesses ranged between STM1-STM64 from a range of sources.

1.4 In order to facilitate analysis, the data was tagged with the geographic location of each IP addresses from the TR-NE research prototype GEOFUSION using `slr-ip-adr-lu-log`.

1.5 The data was parsed to extract client-server and server-client relationships by using the Broadcast-Server and Broadcast-Listener fields that the PPF AEG module output to the single line records.

Analysis

2 Broadcast Population

2.1 There were 224,446 Unique listener IP addresses over the 3 month period covering approximately 108448 /24 subnets.

3 Geographic Distribution of Servers

3.1 Servers were geographically distributed between 1719 individual locations. The Top 50 are shown in Table 1.

Frequency	Location
2237697	PARIS;FR
756510	WESTCHESTER;IE
217796	AMSTERDAM;NL
153888	DUBLIN;IE
146391	KALMAR;SE
125152	MOSCOW;RU
97128	WESTCHESTER;US
85279	PARIS;GB
63901	MILPITAS;US
62837	THEHAGUE;NL
56389	STERLING;US
53432	RIGA;LV
49978	LJUBLJANA;SI
45843	BERLIN;DE
43112	DALLAS;US
41600	FRANKFURT;DE
29308	WARSAW;PL
21199	BUDAPEST;HU
20978	LOSANGELES;US
20687	BUCHAREST;RO
20396	REAL;FR
19495	GOTEBORG;SE
17710	VILNIUS;LT
17065	LONDON;GB
16879	SOFIA;BG
15777	TROY;US
15334	KOLN;DE
14704	POZNAN;PL
13724	HOUSTON;US
12607	KRAKOW;PL
11701	DOSSENHEIM;DE
10913	NURNBERG;DE
10708	CHICAGO;US
10516	ZURICH;CH
9236	BRATISLAVA;SK
8987	STOCKHOLM;SE
8820	COLLEGEPARK;US
8187	ARDEE;IE
7450	MADRID;ES
7184	KIEV;UA
6780	OAKLAND;US
5944	PRAGUE;CZ
4881	SAINTPETERSBURG;RU
4791	MEXICOCITY;MX
4775	PRAHA;CZ
4476	RESTON;US
4448	NEWARK;US
4289	NC;DE
4177	WESTMOLESEY;GB
4072	HAMBURG;DE

Table 1: Top 50 Locations of broadcast servers

3.2 Since GEOFUSION does not provide suitable accuracy for city specific analysis. A breakdown of geographic distribution by country is shown below:

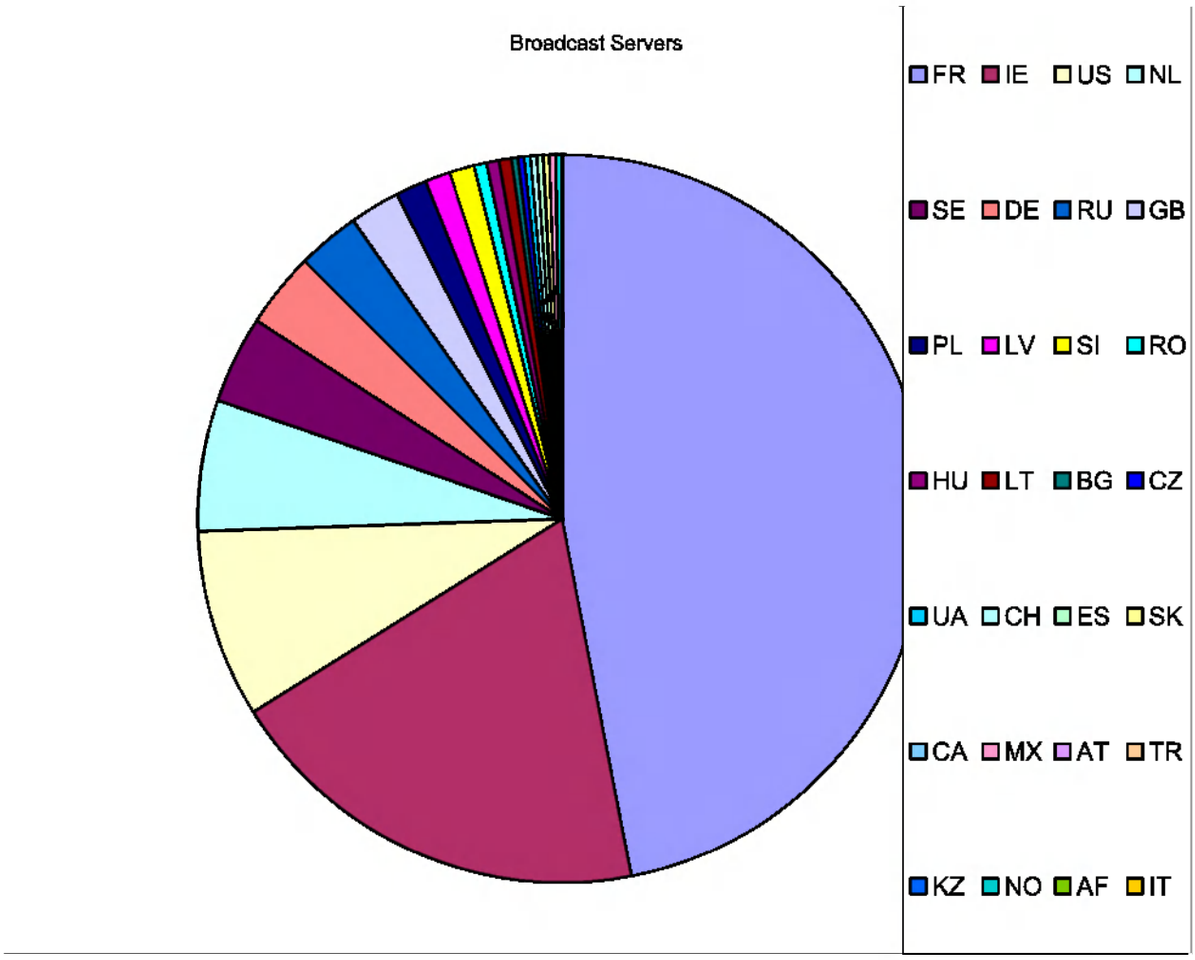

Chart 1: Server location by country

3.3 The top countries of listeners were found to be France, Ireland, the US and the Netherlands, other European countries are also in the Top 10.

Frequency	Country
2261311	FR
918890	IE
396842	US
288907	NL
183631	SE
158202	DE
132895	RU
112180	GB
67145	PL
53516	LV
50833	SI
28308	RO
23010	HU
22620	LT

19517	BG
14183	CZ
13632	UA
12004	CH
11336	ES
9581	SK
6344	CA
5008	MX
4550	AT
3353	TR
3301	KZ
3005	NO
2629	AF
2572	IT
2351	MK
2233	TH

Table 2: Server location by country

Listener Analysis

3.4 The data was analysed to find which country had the most listeners for Internet radio. The top countries were found to be Ireland, Mexico, Japan and the US. However listeners to any one particular radio station could from any of 185 different countries observed. The most frequently seen countries for listeners is shown below:

Frequency	Country
1347162	IE
1006737	MX
824123	JP
486840	US
156282	AN
144270	CA
125266	DE
88647	BR
67825	EC
63618	RO
54953	DO
48473	CO
45494	IL
39594	GB
37187	IR
21557	NL
21489	AU
18990	FR
18510	GR
18149	ES
16957	PK
15015	IT
14554	PL
12637	AE
11092	IN
10330	EG

Table 3: Listener Location by Country

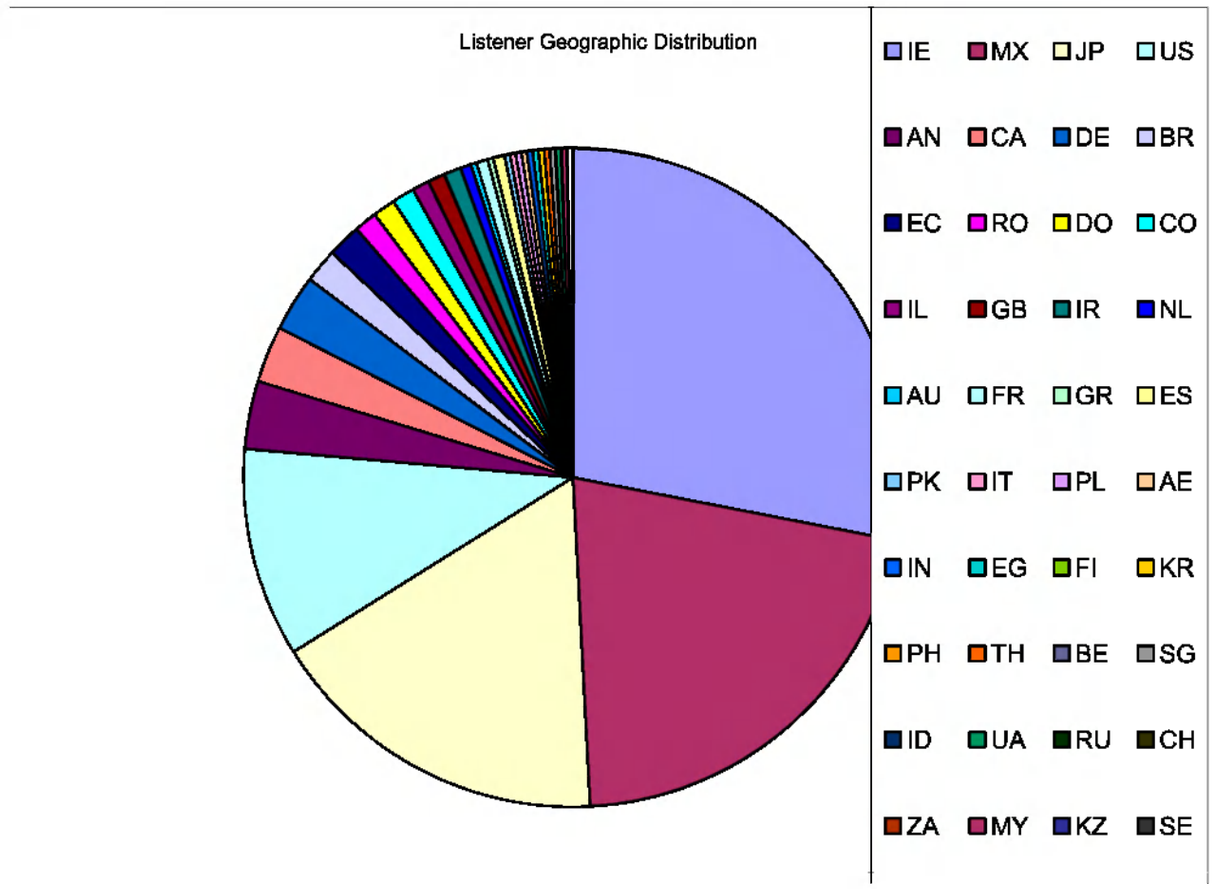

Chart 2: Listener Location by Country

4 Contact Chaining Via Broadcast Events

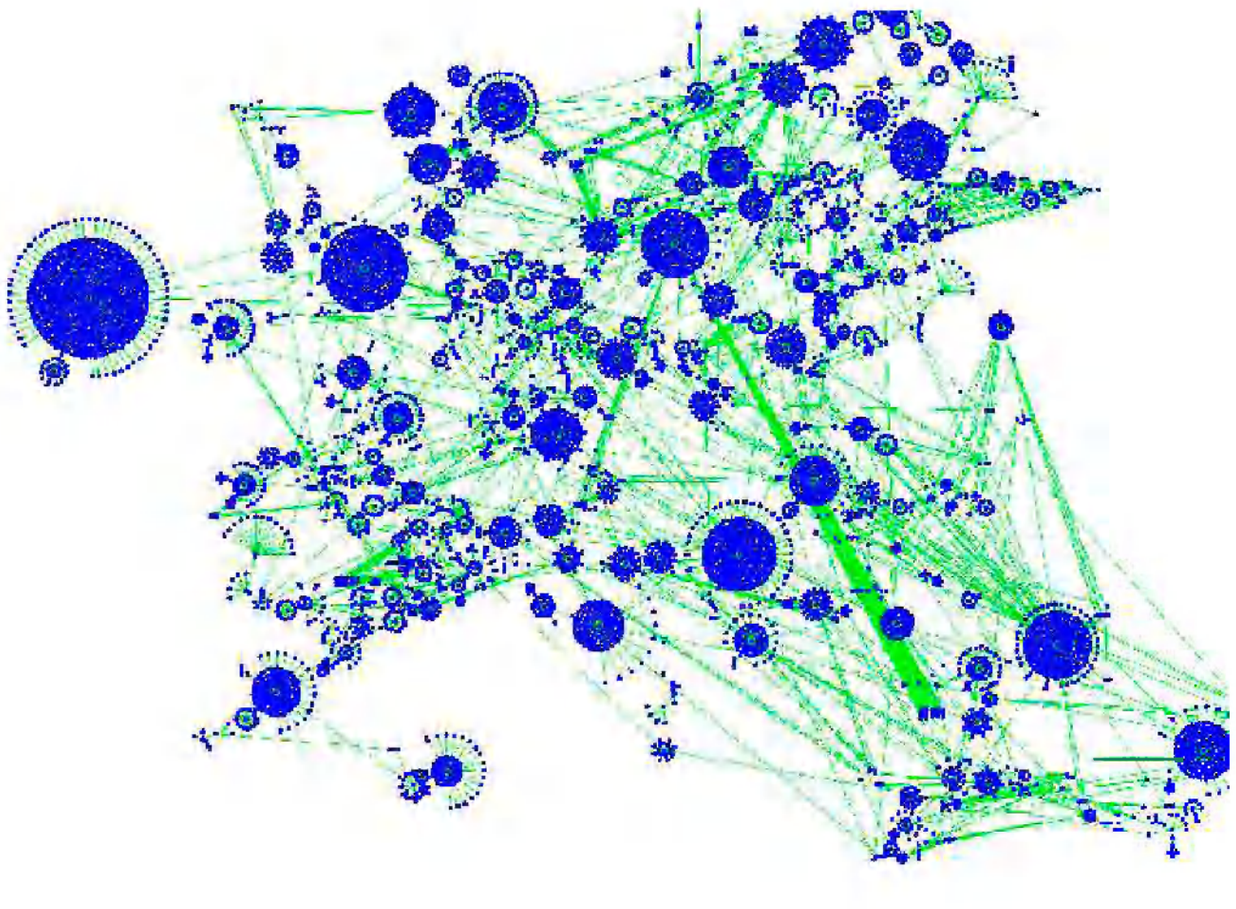

Figure 1: Interconnected Broadcast Events (Renoir)

4.1 Bulk events were visualized in Renoir. Since there is no TDI present within broadcast events, it is difficult to say how many events represent unique users. There were two distinct behaviors exhibited by users of Internet radio stations.

Figure 1 shows the first type – a highly connected group of Internet radio stations with listeners having multiple connections to different radio stations. Figure 2 shows the second trend within the graph. Each radio station has a set of users who are not observed connecting to any other type of Internet radio station.

This observation may be an artifact of the data collection process, which is on a smaller scale than what the corporate architecture can provide. However it may provide an insight into different types of user on the Internet, the technologically savvy user who uses multiple streams of radio for entertainment or news, and a user who knows what they want to listen to.

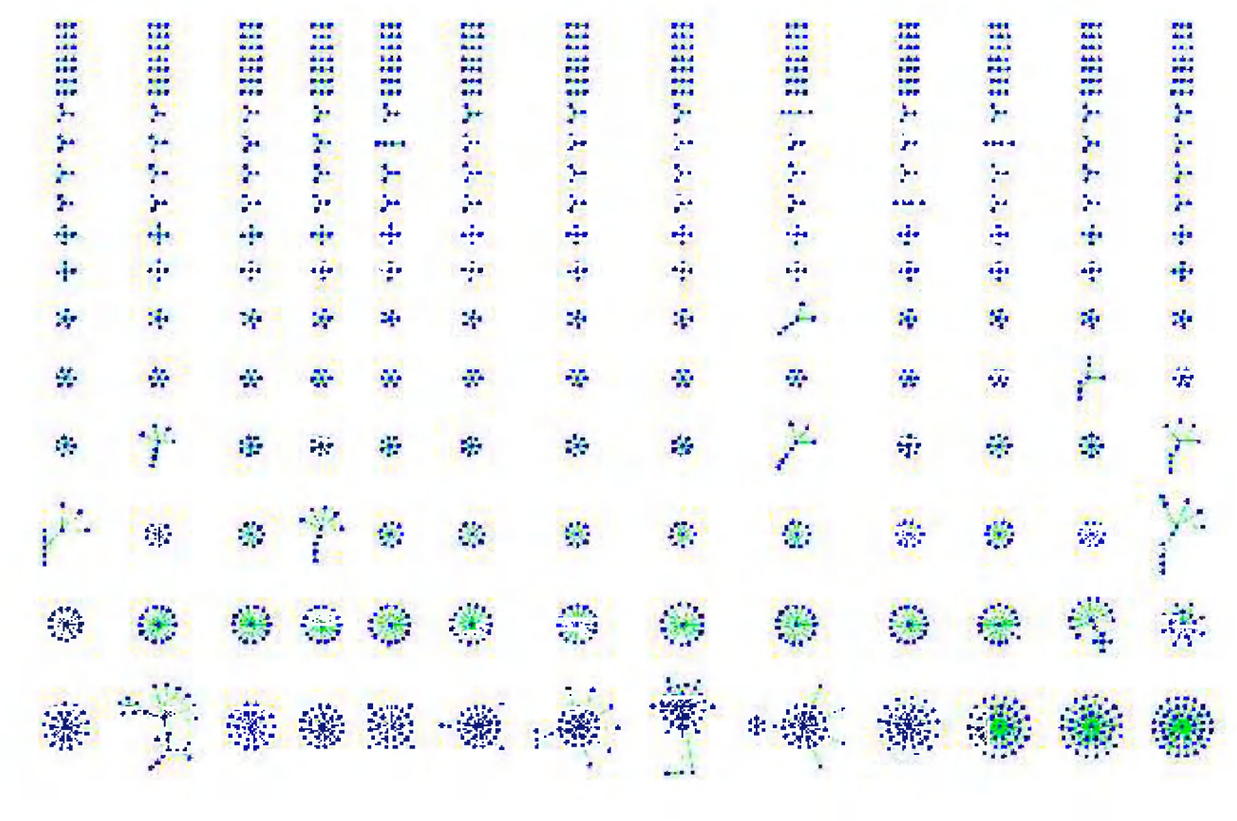

Figure 2: Graphing of broadcast events (Renoir)

5 User Agent Analysis

5.1 The broadcast-client field within the TLVs in the generated data was extracted to see the most common software agents used to listen to Internet radio. The most common software agent was Winamp. A large number of other vendors can be seen. Notably there were nearly 2000 events from users with a PSP (Playstation Portable) and also listening via the Apple iPhone. Internet radio is likely a growth area for mobile phones and mobile devices as wireless networks increase in ubiquity and speed.

Frequency	User-Agent
119711	WinampMPEG
28533	Streamripper
27720	iTunes
14349	RMA
11668	xmms
10594	NSPlayer
10047	MPlayer
8375	BASS
5291	JPlayer
4884	iRAPP
2214	BSPlayer
2137	FreeAmp
2048	Screamer
2025	etAudio
2011	Mozilla
1923	PSP-InternetRadioPlayer

1730	Icecast
1457	tun3rLister
1345	Moodio
1308	VLC
1279	FMOD
1275	Roku
1248	Xine
1147	Today FM Radio Player
1068	Ares
702	GStreamer
603	shoutcastsource
573	Tunin.FM-basic
552	Tunin.FM
538	Apple
470	FStream
405	SN
404	Nullsoft
402	CorePlayer
385	Broadcast-Host
370	SC_iRadio
364	InternetRadioBOX
357	Audacious
353	Internet Explorer
313	vrj
294	RaimaRadio
281	TunInFM
251	Windows-Media-Player
221	iTuner
175	GOGS
168	Shoutcast
168	iPhone
144	gnome-vfs
142	WebRadio
139	ultravox
137	ThereMPEG
137	NSV
131	VirtualRadio
129	Opticodec-PC
129	AIMP2
123	LCG
116	S60InternetRadio
103	RecordTheRadio
98	MyNetRadioPlayer
96	vTuner
94	Resco
89	CodeMorphicAudio
88	PocketTunes
87	FIFMRadio

Table 4: User Agent Frequencies in Data Sample

6 Top Radio Stations by Country

6.1 An analysis was performed on the data in order to see the most popular radio stations in a given country. The following data was obtained:

Country	IP Address	Radio Station
Iran	190.144.31.82	http://www.radiocomunicate.com
Pakistan	174.36.19.83	http://www.cricbuzz.com/
Russia	212.1.226.163	M2 Radio www.m2radio.fr
China	91.121.65.213	http://www.radio-dzair.com
Egypt	207.58.190.16	Radio ISMAILY ON LINE www.shoutcast.com
Zimbabwe	78.157.192.113	www.zeilsteen.com
United Kingdom	88.191.13.53	www.hotmixradio.fr
Netherlands	195.149.107.49	http://www.pueblosoberano.org http://www.newsongsite.com http://www.radiotopfmcuracao.com [Multiple hosted radio stations]
Iraq	72.21.36.210	www.anashed.net
Afghanistan	202.56.179.190	http://www.pamirradio.info
Argentina	208.72.155.18	www.todayfm.com

6.2 Different countries exhibit different behaviours at this level. The top radio stations in Russia and UK are music and entertainment based stations. The top radio station in Iraq appears to be for a Saudi based action group to free prisoners in Iraq.

6.3 It is worth noting that the top radio station in China is a French language Algerian radio station. This is possibly due to inaccuracies in the GEOFUSION dataset or an motivated and interested community in China.

7. Pakistan – UK Connections

7.1 Any potential misuse of the technology could likely include radicalization between Pakistan and the United Kingdom. In order to observe the scale of users in the UK listening to Pakistan based radio stations, or vice versa, the data was filtered to find listeners and servers in the corresponding countries.

7.2 There were 468 events over the 3 month period corresponding to this pattern. These events were picked out and the radio station titles and descriptions were extracted. The most popular stations are shown below.

Goom USA http://www.goomradio.com
Server: 212.23.58.168 Geo: London;GB

RockRadio1.com http://www.rockradio1.com
Server: 78.129.197.4 Geo: London;GB

AWAZ 103.1 FM http://icecast.commedia.org.uk:8000/elcap.mp3
Server: 195.10.228.4 Geo: London;GB

Octane Rollin' http://www.planetdnblive.co.uk
Server: 217.112.93.51 Geo: London; GB

Radio Communicate http://www.radiocomunicate.com
Server: 85.92.197.165 Geo; London; GB

The Eye http://www.103theeve.co.uk
Server: 195.10.228.4 Geo: London;GB

Unity 24 FM http://www.unitv24.org
Server: 195.10.228.4 Geo: London;GB

Radio 1 http://www.radio1.hu
Server 216.66.84.2 Geo: GB [Ambiguous Geofusion Result]
DNS: live.radioramadhansheffield.co.uk

Unknown http://betokun.animenexus.com.mx
Server;216.66.84.2 Geo: GB [Ambiguous Geofusion Result]
DNS: live.radioramadhansheffield.co.uk

Unknown http://www.Simarjot.com
Server: 88.115.99.31 Geo: GB [Ambiguous Geofusion Result]

Surge Live! (Southampton University) http://stream.surge.soton.ac.uk:8000
Server: 152.78.144.108 Geo: Southampton;GB

Radio Party http://www.radioparty.ro
Server: 85.92.197.165 Geo: London;GB

Unknown http://poznan4-2.radio.pionier.net.pl:8000
server: 202.147.163.46 Geo: Gujranwala; PK

Unknown http://v.mccont.com

Server: 92.122.209.33 Geo: London;GB

7.3 These examples are almost exclusively UK based broadcast servers that have listeners in Pakistan. It is not possible to verify the content of each of these audio streams as to whether they match the description given in the URL or Title Field.

7.4 In the case of the Pakistan based broadcast server, the DNS resolves to a domestic ISP LDN. Residential customers can use a dynamic IP address service (such as dyndns) to use their own connection as a static address for a Broadcast audio server.

8. Islamic Radio Stations

8.1 In order to assess the Islamic radicalization risk further, Internet broadcast titles were analyzed for the presence of keywords, Islam and Quran.

8.2 1 record contained the word "Islam" in the "Broadcast-Media-Genre" TLV

8.3 These stations are predominantly broadcasting recitations from the Quran, and represented 4696 events during the survey period.

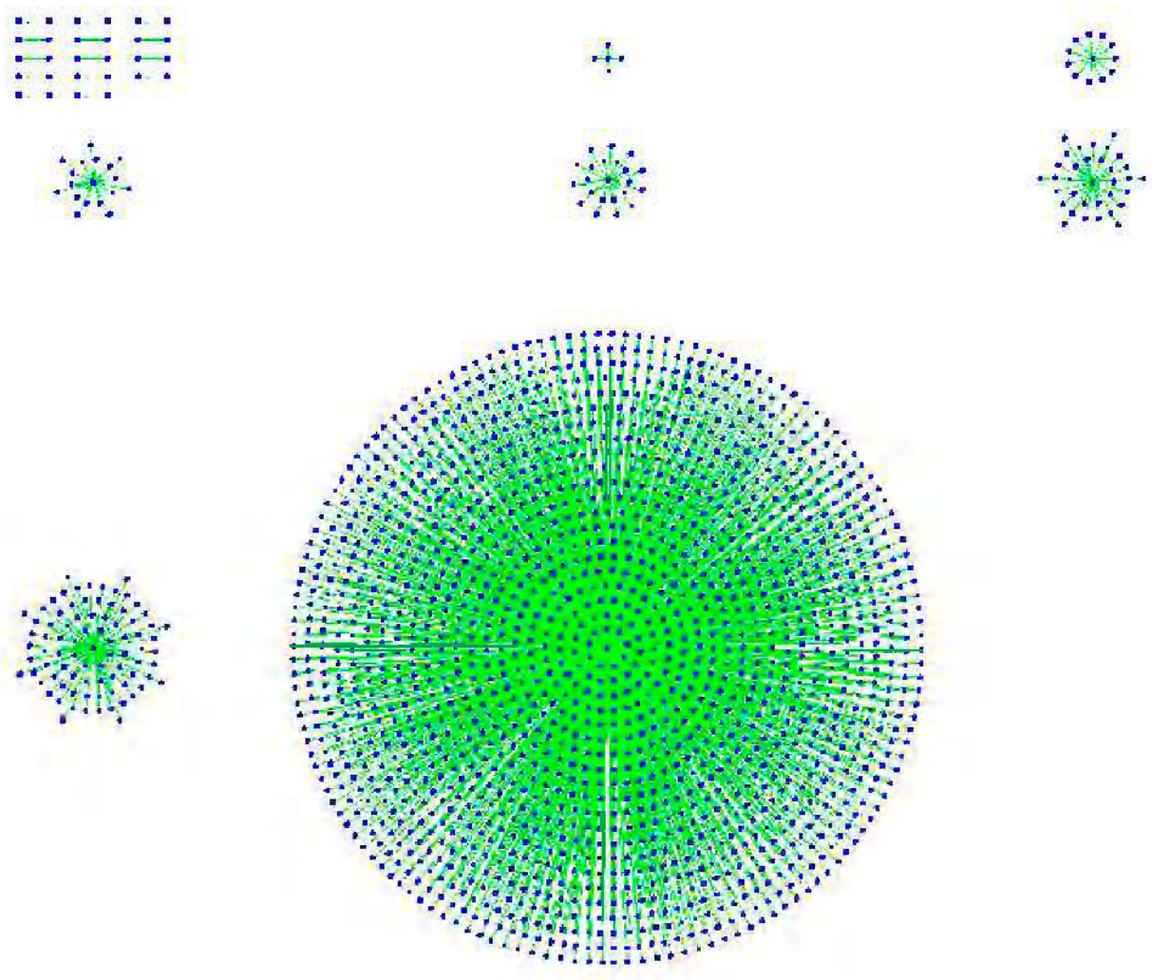

Figure 3: Graphs of top Islamic radio stations (Renoir)

8.4 The following radio stations were identified broadcasting this material. An estimation

of listeners is provided by finding the unique client-server IP pairs seen during the survey.

Jebril http://www.iebril.com

Server: 74.63.225.58 Geo: Dallas;US

1698 Unique Client-Server IP pairs

Audio Islam http://www.audioislam.com:8000

Server: 174.36.1.61 Geo: Dallas;US

81 Unique Client-Server IP Pairs

Radio Dhikr Allah http://dhikr-allah.com

Server: 94.23.215.87 Geo: Paris;FR

4 unique Client-Server IP Pairs

Radio Islam http://radioislam.tv:8000

Server: 87.118.118.66 Geo: Chisinau;DE

11 Unique Client-Server IP Pairs

Dars-E-Quran http://www.darsequran.com

Server: 137.101.32.16 Geo: Karachi;PK

21 Unique Client-Server IP Pairs

Hidayah Online http://aalimraan.hidavahonline.net:8000

Server: 174.36.1.61 Geo: Dallas;US

2 Unique Client-Server IP Pairs

Quranic Audio http://download.quranicaudio.com

Server: 174.36.235.149 Geo: Ashburn;US

1 Unique Client-Server IP Pairs

IslamWeb http://audio3.islamweb.net , http://live.islamweb.net

Server: 202.176.219.164, 205.188.66.157 Geo: Singapore;SG Geo; Reston;US

20 Unique Client-Server IP Pairs

8.5 Case Study and SIGINT Fusion

8.6 As the largest Islamic radio station in the sample, Jebril was chosen as the focus for

some further analysis on its listeners. The Jebril radio station is hosted on 74.63.225.58 and geolocated to Dallas, USA. The radio station has a website associated with it www.iebril.com "The official website of Sheikh Muhammad Jebril". It is a resource for quranic recitations and news.

8.7 The following data was collated for the listeners to this station:

Frequency	Country
491	*Egypt*
478	*Moroocco*
446	*Algeria*
73	*Germany*
56	*US*
43	*Spain*
32	*Iran*
22	*Russia*
20	*Ireland*
18	*Sweeden*
16	*Bosnia & Herzegovnia*
14	*Kazakhstan*
6	*France*
4	*Ukraine*
3	*Sudan*
3	*Netherlands*
2	*South Africa*
2	*Tanzania*
2	*Mauritania*
2	*Italy*
2	*Czech Republic*
2	*Iraq*
1	*Romania*

8.8 In order to understand more about the listeners of any one particular radio station, further bulk SIGINT data from BLAZING SADDLES was used to understand any trends or behaviors.

8.9 KARMA POLICE was able to correlate the Jebril radio station with the TDIs of each of its listeners. This reflected the geographical distribution seen in the broadcast media data with the majority of TDIs geolocating to Egypt and other parts of North Africa.

8.10 This analysis was also performed for TDIs associated with listeners to www.anashed.net the most popular Iraqi radio station in section X.

8.11 The radio stations correlated with 123 distinct Vbulletin users, and users of other technologies such as Skype, Yahoo, MSN and Facebook. Also, it identified listeners of the radio station who use the the Maktoob blogging service.

8.12 A listener was chosen for further Internet profiling. [redacted]@yahoo.com , a user located in Egypt.

8.13 This user was found to have also used the following websites:

Facebook.com
Yahoo.com
Fbcdn.net
amrkhaled.net
e-arabia.com
redtube.com
Youtube.com
ratteb.com
jeeran.com
flickr.com
islamway.com
blogspot.com

8.14 This profile suggests that listeners to Internet radio stations are often users of other Web 2.0 services, also that they use the web to get information from local or non-western news sources, blogs or social media.

9 Recommendations for Future Work

9.1 The single-line-records can be pulled through onto BLACKHOLE to feed a suitable QFD. Since the broadcast results are only events and not TDIs then they need to be correlated with the bulk TDI data that is already being processed. This might benefit Internet profiling work to understand what a user is doing on the Internet (e.g. SAMUEL PEPYS). It could also be adapated into KARMA POLICE to go from a specific radio station to a list of TDIs, or vice-versa.

9.2 This report gives no consideration to the understanding and processing of the audio streams traversing the network. For radio stations that were private, or not accessible by the Internet, this would allow GCHQ to listen to the audio part of the protocol.

9.3 A wealth of datamining techniques could be applied on small closed groups of individuals, to look for potential covert communications channels for hostile intelligence agencies running agents in allied countries, terrorist cells, or serious crime targets.

9.4 An evaluation of Internet radio for future effects operations including information operations in Afghanistan or Iran could be considered as a way of getting rich audio information to a large audience of Internet connected individuals.

10. References

Strategic Framework Task 4134544, 72/09/R/001/C, ICTR