Internet Traffic Misdirection : A Case Study on Belarusian Traffic Diversion and Icelandic Traffic Diversion

Bharath Kumar Reddy Vangoor[1] and Nikhil Mohan[2]

Abstract— **In the recent times, traffic from the financial firms, government agencies, VoIP providers have been a prominent target for getting quietly hijacked and rerouted through ISPs. A sequence of events in which global traffic was redirected to Belarusian ISP GlobalOneBel in Feb 2013 highlights the key point how attackers can misuse the BGP to hijack the routing of traffic off to a another network without the end user having any clue that their traffic was diverted. We use Belarusian Traffic Diversion and the Icelandic Traffic Diversion traffic interception incidents that were observed in Feb 2013 and in July 2013 respectively as a case study to understand : (1) Whether the incidents were accidental or intentional (2) What are the data characteristics to be considered to detect Traffic diversions. (3)Which prefixes may be impacted by traffic interception.[1] To come up with a solution to the above mentioned parameters we will use control plane data(using RouteViews to obtain BGP Updates) to monitor which prefixes may be impacted by traffic interception and validate our technique using data plane traces(using public data sets from iPlane Project and extract trace routes).**

I. Related Work

Using direct observation and active measurement Renesys concluded that various BGP routes were hijacked and as a result some portion of their Internet traffic was misdirected to flow through Belarusian and Icelandic ISPs. Analysis at Renesys, BGP routing data showed evolution of 21 Belarusian events in Feb and May 2013, and 17 Icelandic events in July-Aug 2013. Renesys have active measurements that verify that during the period when BGP routes were hijacked in each case, traffic redirection was taking place through Belarusian and Icelandic routers. These facts were not in doubt; they are well supported by their data.

In contrast to the Renesys, our focus is on analyzing the incidents using only publicly available data to understand what are the data characteristics to be considered to detect internet traffic diversion and to detect whether the incidents were accidental or intentional.

II. Motivation

Practically, Man-In-the-Middle BGP route hijacking has now moved from theory to next level where it can be implemented regularly and making the traffic interception real and easy.[5] Everyone on the Internet, certainly the global carriers like banks,credit card processing companies,government agencies should now monitor their advertised IP prefixes in order to avoid attacks. These kind of attacks should not happen otherwise sensitive data can be extracted and misused. So one of the best way to reduce these attacks is by increasing the transparency. So by coming up with data characteristics that will help to detect traffic interception we can detect the attacks and make them transparent.

III. Methodology

According to Renesys, the traffic redirections took place on an almost daily basis throughout February with the set of victim networks changing daily. Victims whose traffic was diverted varied by day which included major financial institutions, governments and network service providers. There were significant number of live traces to these hijacked networks while the attack was underway. We are trying to find the traces of these path from the data plane measurements and control plane measurements. The two major examples of a trace we are going to conduct our study is based on Belarusian Traffic Diversion and Icelandic Traffic Diversion. Let us split our analysis with respect to these two traffic diversions:

A. Pre-Knowledge

To start with, we have the destination Ip address from the Renesys which experienced several traffic redirections. [2] We use the fact that the Ip prefix has to remain same for a particular Ip address at any given point of time. The Ip prefix can be extracted from the cymru website using the command: (whois h whois.cymru.com -v 63.234.113.110).[6] We use this Ip prefix of the destination to extract the required data from the humongous internet data. This extracted data represents those which has the intended destination that is experiencing the hijack and all the possible sources to this destination. So there is a high probability of hitting on a single AS path that would deviate from the usual defined path in case of a hijack. This is done through the AS path comparisons at the prefix level as the prefix of this destination has to remain same on any day.

In the world of BGP, each routing domain is known as an autonomous system, or AS. What BGP does is help choose a path through the Internet, usually by selecting a route that traverses the least number of autonomous systems: the shortest AS path. To use BGP we would need an AS number, which we can get from the American Registry of Internet Numbers (ARIN).Once BGP is enabled, the router will pull a list of Internet routes from its BGP neighbors. It will then scrutinize them to find the routes with the shortest AS paths. These will be put into the router's routing table.

[1] V. Bharath is with Department of Computer Science Engineering, Stony Brook University,NY 11790, USA `bvangoor at cs.stonybrook.edu`

[2] Nikhil is with the Department of Computer Science Engineering, Stony Brook University,NY 11790, USA `nmohan at cs.stonybrook.edu`

Generally, but not always, routers will choose the shortest path to an AS. BGP only knows about these paths based on updates it receives. Unlike Routing Information Protocol (RIP), a distance-vector routing protocol which employs the hop count as a routing metric, BGP does not broadcast its entire routing table. At boot, the peer will hand over its entire table. After that, everything relies on updates received. Route updates are stored in a Routing Information Base (RIB). A routing table will only store one route per destination, but the RIB usually contains multiple paths to a destination. It is up to the router to decide which routes will make it into the routing table, and therefore which paths will actually be used. In the event that a route is withdrawn, another route to the same place can be taken from the RIB.[9]

The RIB is only used to keep track of routes that could possibly be used. If a route withdrawal is received and it only existed in the RIB, it is silently deleted from the RIB. No update is sent to peers. RIB entries never time out. They continue to exist until it is assumed that the route is no longer valid. The below analysis is based on this pre-knowledge which describes the procedure adopted to gain this knowledge and apply it accordingly on 2 different traffic diversion scenarios.

B. Belarusian Traffic Diversion

To characterize the events that took place in Belarusian Traffic Diversion interception incidents on Feb 2013, we use a combination of publicly available control and data-plane measurements. We have used the data plane measurement as the first step towards analyzing the Belarusian Traffic Diversion.

Data-plane Measurements:

We use data-plane measurements from the iPlane project[3] and follow the below steps to analyze the data:

1) We use the 'wget script' and download all the traceroute files of the date before the hijack, on the day of hijack and the date after the hijack from the iPlane project ($http : //iplane.cs.ucr.edu/iplane_{l}ogs/$).[8]
2) We parse the files downloaded from the iPlane using the parser (Parse.c) and extract the destination Ip, number of hops, source to destination Ips with their RTT (Round Trip Time) and TTL (Time to Live).
3) From the Pre-Knowledge as discussed we can compute the prefix of the given Ip address. The destination Ip of Belarusian Traffic Redirection is '63.234.113.110'. The prefix calculated for this Ip is : '63.224.0.0/12'. This shows that the first 12 bits of the Ip does not change and the remaining bits of the Ip changes. So we use this fact and deduce that the first 8 bit number in the Ip is always same i.e '63' which will be used in the next step to filter the data and get the required Ips.
4) We used the script (Script.sh) that uses the blend of 'cat', 'awk' and 'grep' to separate out the required Ips according to step 3 from the files for each of the dates (i.e. date before the hijack, on the day of hijack and the date after the hijack).
5) The step 4 dumps all the required source to destination Ips to a single file. We pass this file that contains the list of Ips to cymru website to get the AS Number, prefix of the Ip, location using the script (netcat whois.cymru.com 43 <InputFile.txt >OutputFile.txt). Here 'InputFile.txt' contains list of Ips and 'OutputFile.txt' contains the Ip, its AS Number, prefix of the Ip.
6) Now we have to analyze the AS paths in the files whose prefixes match between the different days.

Below is one of the sample format of the refined data of data plane measurement which shows the Source and destination Ip with their AS number. The AS numbers in the below table represents the AS path that needs to be analyzed for the prefix '63.224.0.0/12':

Data Plane Measurement for Belarusian Traffic Diversion		
ASN Number	Ip Address	Prefix
Source:10326	75.130.96.1	75.130.96.0/24
174	38.104.218.5	38.0.0.0/8
174	66.28.4.221	66.28.0.0/16
174	154.54.25.113	154.48.0.0/12
174	154.54.47.218	154.48.0.0/12
174	154.54.11.190	154.48.0.0/12
2828	207.88.14.185	207.88.0.0/16
2828	207.88.12.9	207.88.0.0/16
2828	207.88.12.2	207.88.0.0/16
2828	216.156.0.82	216.156.0.0/16
2828	71.5.180.3	71.4.0.0/15
40621	209.117.12.1	209.117.12.0/23
Destination:209	63.234.179.1	63.224.0.0/12

Table 1: Sample data plane measurement

The analysis can be described as below by taking the example from the Renesys website for the Belarusian Traffic Redirection:

We first map each Ip in the traceroute to the AS originating the closest covering prefix at the time of the trace route. This is done by searching for the destination Ip prefix '63.224.0.0/12' (Washington) from the refined data that is available. Once we attain the pair, we check for the AS path of source to destination. Now we compare the AS path of 3 days to confirm if there is any suspicious behavior. The original path was intended to move from Guadalaraja, Mexico to Washington, DC on Feb 27th. If we observe trace route AS-path that does not contain UK, Moscow on Feb 26th and Feb 28th but if it is available on Feb 27th then we can conclude that the trace route was intercepted. That is because the traffic redirection happened just for a couples of minutes or just for a single day.[2][4]

Control Plane Measurements:

Using Destination Prefix: We use Routeviews monitors as a source of BGP updates from around the time of attack. We follow the below steps to analyze the data:

1) We use the wget script and download all the route view files of the date before the hijack,

on the day of hijack and the date after the hijack from the University of Oregon Route Views (http://archive.routeviews.org/bgpdata/).[7] The format that is downloaded is MRT format RIBs.

2) We parse the downloaded files using the bgpdump.c and extract the prefix, sequence, source, origin, As Path and next hop.
3) From the Pre-Knowledge as discussed we know the prefix of the destination. The prefix for the destination Ip is '63.224.0.0/12'. We use the scripts to separate out the required Ips for each of the dates (i.e date before the hijack, on the day of hijack and the day after the hijack)
4) The step 3 creates a required file which contains the required Ip, its prefix, As Path that needs to be analyzed.

Below is the sample format of the partial refined data of control plane measurement which shows the various information like: prefix, sequence, origin, AS Path, Next Hop etc.

Control Plane Measurement for Belarusian Traffic Diversion	
Attributes	Values
PREFIX	63.224.0.0/12
SEQUENCE	53521
FROM	91.209.102.1 AS39756
ORIGIN	IGP
ASPATH	39756 3257 209
NEXTHOP	91.209.102.1

Table 2: Control plane data (Using destination Prefix)

The analysis will mainly involve the AS path of the prefixes. From the above table we concentrate on the ASPATH row that shows the AS numbers that are involved with prefix '63.224.0.0/12' as the destination.

The AS path of the prefixes are compared between the dates and is checked for any suspicious behavior. The traffic diversion can be witnessed if there is any unusual path taken for same prefix other than the common path.

Using Hijacked Prefix: Hijacked AS is given in the Renesys website. Even for this method, we use Routeviews monitors from around the time of attack. We followed the below steps to analyze the data:

1) We use the wget script and download all the route view files of the date before the hijack, on the day of hijack and the date after the hijack from the University of Oregon Route Views (http://archive.routeviews.org/bgpdata/). The format that is downloaded is MRT format RIBs.
2) We parse the downloaded files using the bgpdump.c and extract the prefix, sequence, source, origin, As Path and next hop.
3) Now we consider the hijacked AS to refine our search i.e hijacked AS : AS28849.
4) Using this AS number as input, find all the possible AS paths related to this AS number and the prefixes registered to this hijacked prefix.
5) Collect this data for the day before the hijack, on the day of hijack.

Below is the sample format of the refined control plane measurement which shows information on the AS path through hijacked AS or hijacked 'AS' as the destination with the prefixes registered under the hijacked AS.

Control Plane Measurement for Belarusian Traffic Diversion	
AS Path	Registered Prefix
701 3356 6697 28849	185.15.156.0/22
1668 3356 6697 28849	185.15.156.0/22
286 3356 6697 28849	185.15.156.0/22
7660 4635 20485 6697 28849	185.15.156.0/22
3549 20485 6697 28849	185.15.156.0/22
11686 11164 9002 6697 28849	185.15.156.0/22
6762 3356 6697 28849	217.23.119.0/24
1221 4637 3356 6697 28849	217.23.119.0/24
6762 3356 6697 28849	217.23.121.0/24
1668 3356 6697 28849	217.23.122.0/24

Table 3: Control plane data (Using Hijacked AS)

The analysis will mainly involve the prefixes registered under the hijacked AS. In the above table, the last AS under AS Path column is the hijacked AS in every row of the table. The prefixes registered under this hijacked AS is compared between the days to check if there is any anomaly i.e difference in number of registered prefixes. If there is difference in number of registered prefixes, then the differed prefixes are analyzed to check if those are hijacked. That is done by checking the sub-prefixes as well.

C. Icelandic Traffic Diversion

Like the Belarusian Incident, we use the data plane and control plane measurements to prove the Icelandic Traffic Diversion as well. The events spread over the period of July 31st to 19th of August. From the Renesys website we have a catch that shows the trace route passing via Iceland which was intended to move to Denver, Colorado from Denver, Colorado. We have used the data plane measurement as the first step towards analyzing the Icelandic Traffic Diversion.

Data-Plane Measurements:

1) Follow the steps 1,2 as mentioned in the Data-Plane measurements of Belarusian Traffic Diversion.
2) From the Pre-Knowledge as mentioned we can compute the prefix of the given Ip address. The destination Ip of Icelandic Traffic Redirection is 206.51.69.201. The prefix calculated for this Ip is : '206.51.64.0/20'. This shows that the first 20 bits of the Ip does not change and the remaining bits of the Ip changes. So we use this fact and deduce that the first 16 bit number in the Ip is always same i.e 206.51 which will be used in the next step to filter the data and get the required Ips.
3) We follow the step 4,5,6 as mentioned in the data plane measurement in Belarusian Traffic Diversion.

Below is the sample format of the refined data of data plane measurement which shows the Source and destination Ip with their AS number. The AS number in between these represents the AS path that needs to be analyzed for the prefixes '206.51.64.0/20':

Data Plane Measurement for Icelandic Traffic Diversion		
ASN Number	Ip Address	Prefix
Source:22561	208.110.248.30	208.110.240.0/20
22561	208.110.248.33	208.110.240.0/20
13341	74.118.8.171	74.118.8.0/21
13341	206.51.67.254	206.51.66.0/23
11351	72.43.89.1	72.43.64.0/19
11351	24.58.150.80	24.58.0.0/15
7843	66.109.6.74	66.109.0.0/20
7843	66.109.6.26	66.109.0.0/20
10796	65.189.180.49	65.189.128.0/18
11427	24.175.56.73	24.175.0.0/17
11427	24.175.56.69	24.175.0.0/17
3356	4.68.63.21	4.0.0.0/9
3356	4.69.142.186	4.0.0.0/9
137	193.206.137.66	193.206.0.0/16
137	90.147.80.189	90.147.0.0/16
3549	208.50.25.117	208.50.0.0/17
3549	67.16.147.30	67.16.0.0/15
22561	206.51.69.65	206.51.64.0/20
22561	206.51.69.196	206.51.64.0/20
22561	206.51.69.10	206.51.64.0/20
Destination:22561	206.51.69.199	206.51.64.0/20

Table 4: Sample data plane measurement

The analysis of data plane measurement for this case study remains same as Belarusian Traffic Diversion, only the change being the dates taken into the consideration and the source and destination for the analysis.

Control Plane Measurements:

Using destination Prefix: We use Routeviews monitors as a source of BGP updates from around the time of attack.

Follow the steps 1,2,3,4 as mentioned in the control plane measurement in Belarusian Traffic Diversion. The only change here is the destination Ip prefix (206.51.64.0/20) and the location.

Below is the sample format of the partial refined data of control plane measurement which shows the various information like: prefix, sequence, origin, AS Path, Next Hop etc.

Control Plane Measurement for Icelandic Traffic Diversion	
Attributes	Values
PREFIX	206.51.64.0/20
SEQUENCE	420825
FROM	213.144.128.203 AS13030
ORIGIN	IGP
ASPATH	13030 2828 209 22561
NEXTHOP	213.144.128.203

Table 5: Control plane data (Using destination Prefix)

The analysis will involve the study of AS paths over the range of the dates.(Data before the hijack, on the day of Hijack and after the day of Hijack).

Using Hijacked Prefix: We use Routeviews monitors from around the time of attack to monitor the hijacked prefix.

Follow the steps 1,2,3,4,5 as mentioned in the control plane measurement (Using hijacked Prefix) in Belarusian Traffic Diversion. The only change here is the hijacked AS (AS48685) and the location.

Below is the sample format of the refined control plane measurement which shows information on the AS path through hijacked AS or hijacked 'AS' as the destination with the prefixes registered under the hijacked AS for Icelandic events.

Control Plane Measurement for Icelandic Traffic Diversion	
AS Path	Registered Prefix
1668 3257 6677 48685	94.142.152.0/21
1221 4637 174 6677 48685	94.142.152.0/21
293 6453 12969 48685	94.142.152.0/21
2914 174 6677 48685	185.25.252.0/22
1239 3257 6677 48685	176.10.32.0/21
8492 9002 6677 48685	176.10.32.0/21
701 3257 6677 48685	185.25.252.0/22
701 3257 6677 48685	185.25.252.0/22
11686 19151 6677 48685	185.25.252.0/22
3561 3257 6677 48685	185.25.252.0/22
3257 6677 48685	185.25.252.0/22

Table 6: Control plane measurement (Using hijacked AS)

The analysis will involve the study of the prefixes registered under the hijacked AS over the days before hijack and during the hijack to fetch the anomaly.

Data Plane Measurements for impact analysis:

Using Hijacked AS: We have used the data plane measurement to find out the affected countries due to Belarusian and Icelandic incidents. Below are the steps followed to find out the affected countries :

1) We will have the hijacked prefixes for each of the incident which can be used to extract the traceroute information from the data plane measurement.
2) Now all the possible sources to this hijacked prefix is extracted.
3) The countries of these sources are taken into consideration.
4) These are the most probable countries to get affected because of the Belarusian and Icelandic hijack.

The analysis includes the the total number of each countries involved in the path of the hijacked AS with respect to total number of available prefixes on the particular day of hijack as the measurement. This is pictured as the graph and is shown in the result.

Below is the sample refined data that gives complete information of a particular prefix for one traceroute with the hijacked Prefix as the destination.The source in the below traceroute is AS10326 and the destination is AS9286.

Data Plane Measurement for impact analysis				
AS	IP	IP-Prefix	Registered Country	Registered Organization
10326	75.130.96.1	75.130.96.0/24	US	WPI - Worcester Polytechnic Institute,US
10578	207.210.142.141	207.210.142.0/24	US	GIGAPOP-NE - Harvard University,US
11164	64.57.21.209	64.57.20.0/23	US	INTERNET2-TRANSITRAIL-CPS - Internet2,US
11164	64.57.20.196	64.57.20.0/23	US	INTERNET2-TRANSITRAIL-CPS - Internet2,US
11164	64.57.20.247	64.57.20.0/23	US	INTERNET2-TRANSITRAIL-CPS - Internet2,US
9318	58.229.15.105	58.224.0.0/13	KR	HANARO-AS Hanaro Telecom Inc.,KR
9318	210.180.97.174	210.180.96.0/19	KR	HANARO-AS Hanaro Telecom Inc.,KR
9318	110.13.128.66	110.13.0.0/16	KR	HANARO-AS Hanaro Telecom Inc.,KR
9286	203.246.170.34	203.246.168.0/22	KR	LGH-AS-KR LGHitachi,KR
9286	202.68.254.1	202.68.224.0/19	KR	LGH-AS-KR LGHitachi,KR

Table 7: Data plane measurement (Using hijacked AS)

D. Results

Out of the several ways tried out to check the hijack, the method of extracting the registered prefixes of the hijacked AS from the control plane measurement gave us the way to prove the hijack. Below is the result for each method.

1) Data Plane Measurement: The traceroute extracted from the Renesys website to crosscheck the hijack was not visible in the data pane measurement for both Belarusian and Icelandic incidents since the traceroute was specific hijacked path given by Renesys.

2) Control Plane Measurement Using Destination Prefix: This method gave us all the possible AS path for the destination prefix as defined in Table 6. But the limitation of the paths being the data available only from the level 3 routers and it was not sufficient to find the hijacked AS. So the hijacked AS stayed hidden.

3) Control Plane Measurement Using Hijacked AS: This methodology of using the hijacked AS exposed the proof by showing the differences in the number of prefixes registered to the hijacked prefixes. This is proved only after checking the sub-prefixes of the hijacked prefixes.

Below is the data supporting the various scenarios.

Prefixes registered for Belarusian during hijack	
Number of occurrences	Registered Ip Prefix
384	185.15.156.0/22
384	217.23.112.0/20
372	217.23.112.0/24
372	217.23.113.0/24
372	217.23.114.0/24
372	217.23.115.0/24
372	217.23.116.0/24
6	202.68.224.0/19
372	217.23.117.0/24
372	217.23.118.0/24
372	217.23.119.0/24
372	217.23.120.0/24
372	217.23.121.0/24
372	217.23.122.0/24
372	217.23.123.0/24
372	217.23.124.0/24
372	217.23.125.0/24
372	217.23.126.0/24
372	217.23.127.0/24

Table 8: Prefixes registered for Belarusian during hijack

The number of registered prefixes to the hijacked AS of Belarusian incident before the hijack is : 17 and during the hijack is 18. The additional prefix during the hijack (202.68.224.0/19 : highlighted in the table) which was advertised as Belarusian originally belongs to Korea. For this incident there is no sub-prefixes to check. So this anomaly proves the Belarusian Hijack.

Prefixes registered for Icelandic before hijack	
Number of occurances	Registered Ip Prefix
372	176.10.32.0/21
372	185.25.252.0/22
372	94.142.152.0/21

Table 9: Prefixes registered for Icelandic before hijack

The number of registered prefixes to the hijacked AS of Icelandic incident before the hijack is 3 and during the hijack is 600. The additional 597 prefixes during the hijack belong to US .

Below table shows the prefixes registered during the hijack for Icelandic event. Due to space constraint, not all prefixes are shown.

Prefixes registered for Icelandic during hijack	
Number of occurances	Registered Ip Prefix
372	176.10.32.0/21
372	185.25.252.0/22
372	94.142.152.0/21
8	209.87.79.0/24
8	216.151.248.0/24
12	216.231.34.0/24
.	.
.	.
.	.
597 anomaly prefixes in total	

Table 10: Prefixes registered for Icelandic during hijack

There are 6 sub-prefixes advertised as part of hijacked prefixes. And these prefixes are also hijacked. That is proved by checking the original location of sub-prefix with respect to their prefixes. So this anomaly proves the Icelandic Hijack.

Table 11 shows all the sub-prefixes that were hijacked for Icelandic event.

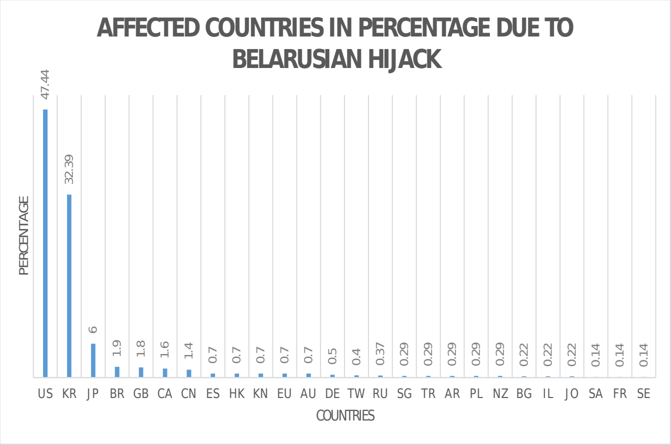

Fig. 1. Affected countries in percentage due to Belarusian Hijack

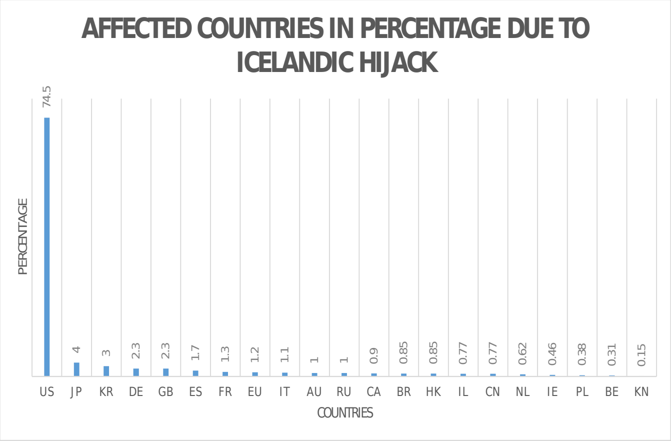

Fig. 2. Affected countries in percentage due to Icelandic Hijack

Sub-prefixes registered for Icelandic during hijack	
Number of occurances	Sub-Prefix
7	216.27.128.0/19
8	64.81.192.0/19
1	66.92.240.0/23
1	66.93.216.0/21
1	66.93.224.0/22
1	74.82.100.0/22

Table 11: Sub-prefixes registered for Icelandic during hijack

Data Plane Measurements for impact analysis:

Using Hijacked AS: After the analysis of the total number of each impacted countries with respect to the total number of countries involved on the day of the hijack, below is the result derived for each of the incidents.

Figure 1 gives the percentage distribution of probable impacted countries during the Belarusian hijack.

Figure 2 gives the percentage distribution of probable impacted countries during the Icelandic hijack.

The highest impact is borne by the US,Korea etc. in Fig 1 and US,Japan etc. in Fig 2 because these countries were directly involved in the path moving towards the hijacked AS and have the highest traffic moving towards the hijacked AS. All the other countries are also analyzed and the percentage is shown in the graph for every country affected due to hijack.

E. Future Work

The results that is accumulated from the above scenarios proves the hijack at Belarus and Iceland. This study can be expanded to expose more hidden BGP hijacks and reduce these attacks by bringing transparency.[2] The impacted countries can be analyzed more to narrow down on the customers and ISPs directly affected due to these events. The scenarios used in this paper can be tweaked to understand the paths taken by the traffic of various ISPs and can be geographically mapped to understand the ISP relations.

REFERENCES

[1] R Hiran,N Carlsson, and P Gill. ”Characterizing Large-scale Routing Anomalies: A Case Study of the China Telecom Incident”

[2] J Cowie. Renesys blog: ”The New Threat: Targeted Internet Traffic Misdirection. http://research.dyn.com/2013/11/mitm-internet-hijacking/#!prettyPhoto”

[3] Harsha V. Madhyastha, Ethan Katz-Bassett, Thomas Anderson, Arvind Krishnamurthy and Arun Venkataramani. ”iPlane: An Information Plane for Distributed Services” http://iplane.cs.washington.edu

[4] Internet Society: ”BGP Hijacking In Iceland And Belarus Shows Increased Need for BGP Security”. http://www.internetsociety.org/deploy360/blog/2014/02/bgp-hijacking-in-iceland-belarus-shows-increased-need-for-bgp-security/

[5] Jaikumar Vijayan. Computer World: ”Warning! Targeted Internet misdirection on the rise”. http://www.computerworld.com/article/2486076/security0/warning–targeted-internet-misdirection-on-the-rise.html

[6] Cymru Ip to ASN Lookup : http://asn.cymru.com/cgi-bin/whois.cgi

[7] Route View Data : http://archive.routeviews.org/

[8] iPlane Data : $http : //iplane.cs.ucr.edu/iplane_logs/$

[9] BGP Updates Info : http://www.enterprisenetworkingplanet.com /netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm/