



HURRICANE ELECTRIC
INTERNET SERVICES

Misused Top ASNs

Analysis of AS1, AS2 and AS3 misuse!

Officially allocated to...

AS 1 - Level3 Communications

AS 2 - University of Delaware

AS 3 - MIT

November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

How they are “leaked” ?

November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Reasons for leak...

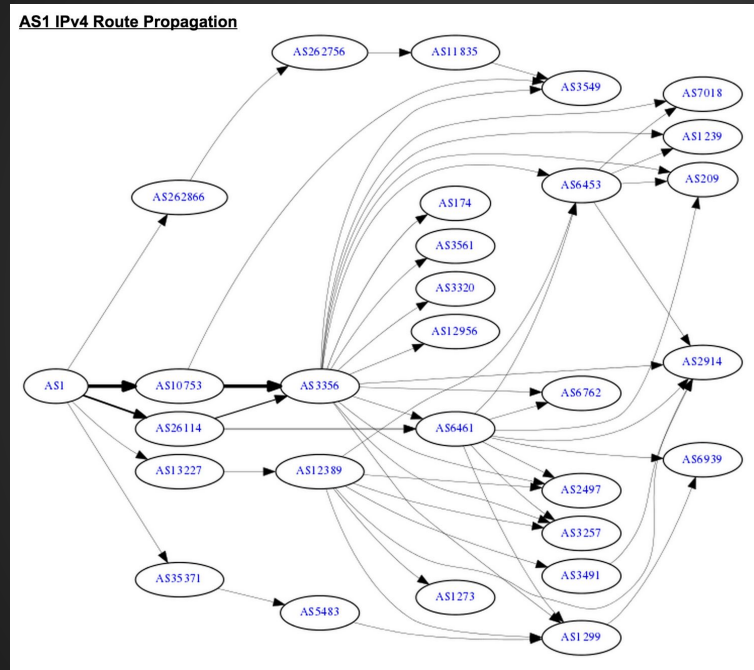
- “Copy-paste” of sample prepend configuration “1 2 3”
- Mistakenly typing “1 2 or 3” in prepend rules in route filter / export policy statement

Impact of leak

Hard to determine statistically but ...

- Shows unexpected relationship of leaking AS with top ASN and among top ASNs!
- Considered to be “AS hijack” and bad for trust based BGP routing
- Can result in (wrongly prepended) announcement getting filtered across parts of internet
- Chances of broken connectivity of these routes with top ASNs network due to BGP loop prevention

AS1 Graph V4



AS1 Peer V4

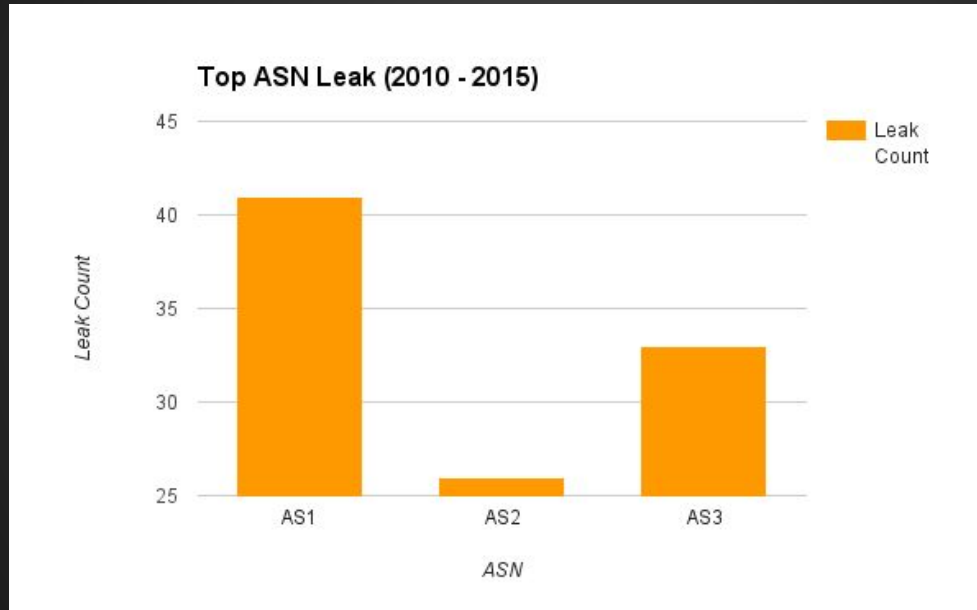
Rank	Description		IPv6	Peer
1	Level 3 Communications, Inc.			<u>AS10753</u>
2	Anaplan, Inc.			<u>AS26114</u>
3	Kraft-S JSC			<u>AS13227</u>
4	Softkit SRL			<u>AS35371</u>
5	TURBO 10 Telecomunicaes Ltda.			<u>AS262866</u>
6	Internet2			<u>AS11537</u>
7	Fibercut SRL			<u>AS43647</u>
8	OANTA SRL			<u>AS44912</u>
9	PAN-NET SRL			<u>AS42405</u>
10	National Exchange Carrier Association, Inc.			<u>AS21616</u>

November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Hunting for leakers...

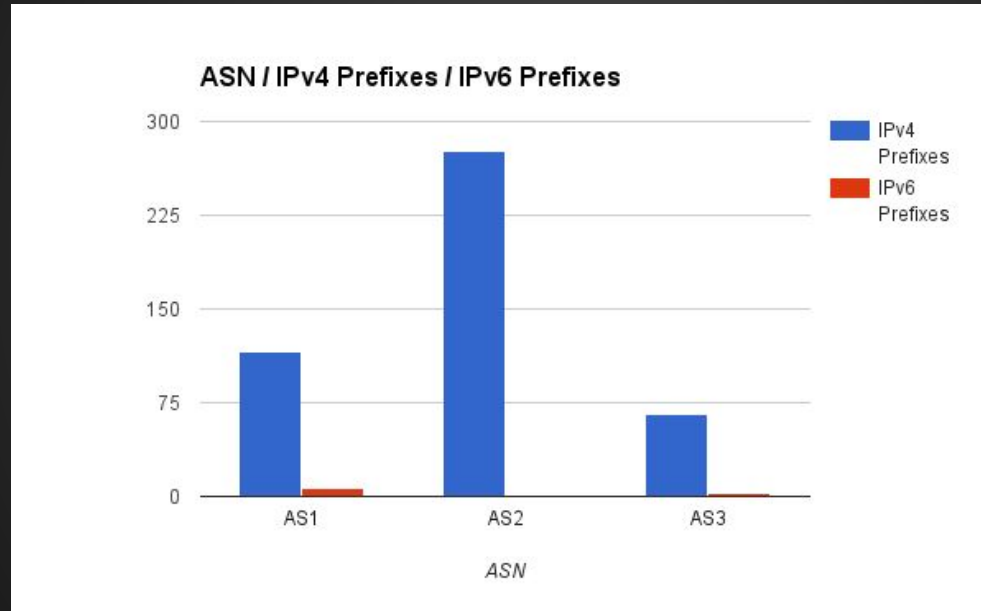
- Analysis of routing table from multiple RIPE RIS collectors
- Analysis from 2010 to 2015
- Looking for cases where top ASNs appear in AS_PATH for routes which belong to other ASNs.
- Focus of top ASNs appearance with prepends in the routing table
- Assumption that except AS1, other two top ASNs aren't transit provider (since belonging to University)
- Leaks which appeared for less than 24hrs are not collected

Distribution of appearance



November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Distribution of leaks (IPv4 Vs IPv6)



Some of who leaked AS1...

AS Number	Start Date	End Date	Visibility in days
5927	22-Jul-2011	3-Dec-2011	134
7046	9-May-2010	11-Jun-2010	33
14758	25-Apr-2013	20-Jun-2013	56
21011	28-Jan-2013	5-Feb-2013	8
21219	28-Jan-2013	5-Feb-2013	8
26114	11-Jun-2013	22-Jul-2015	771
35819	23-Nov-2014	26-Nov-2014	3
40807	7-Jan-2010	24-Apr-2010	107
45899	1-Dec-2014	17-Apr-2015	137
49994	26-Nov-2013	29-Nov-2013	3
50113	31-May-2013	8-Jun-2013	8
51282	3-Nov-2010	19-Nov-2010	16
52931	3-Nov-2010	19-Nov-2010	16
55836	24-Nov-2014	26-Nov-2014	2

November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Some of who leaked AS2...

AS Number	Start Date	End Date	Visibility in days
12989	14-Oct-2014	26-Oct-2014	12
131211	19-May-2015	22-Jul-2015	64
131713	20-Apr-2015	4-Jun-2015	45
133219	6-Jul-2015	22-Jul-2015	16
17483	30-Jun-2010	7-Jul-2010	7
17658	7-Feb-2014	18-May-2015	465
197706	22-Sep-2011	25-Oct-2011	33
197790	7-Apr-2014	3-Jun-2014	57
197798	18-Jul-2013	26-Aug-2013	39
198040	2-Jan-2015	2-Feb-2015	31
23951	1-Feb-2011	23-Apr-2011	81
262587	29-May-2013	7-Jun-2013	9
262878	20-Aug-2011	25-Aug-2011	5
263042	17-Jul-2013	23-Aug-2013	37

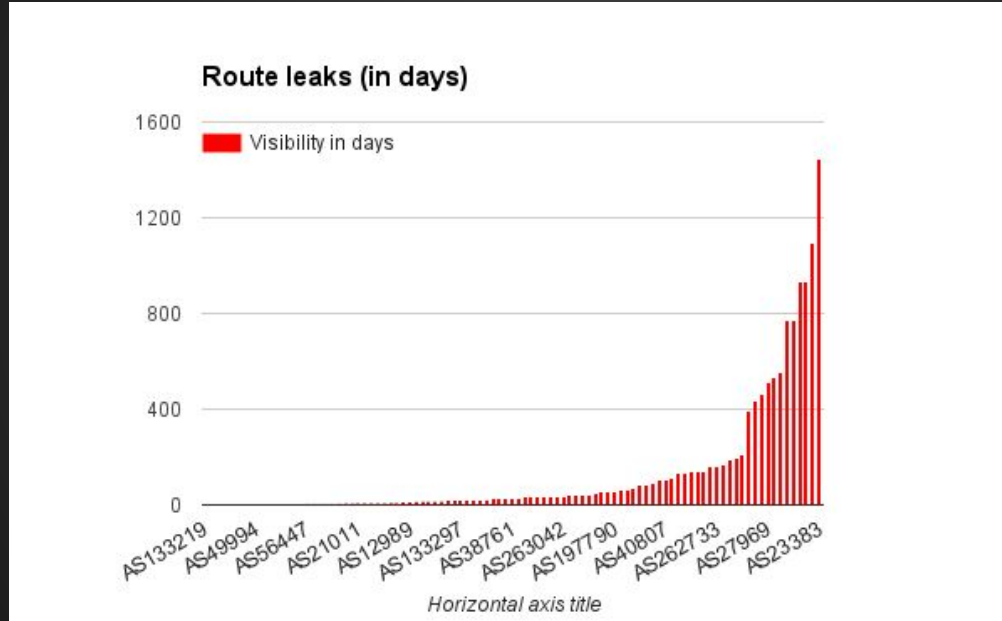
November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Some of who leaked AS3...

AS Number	Start Date	End Date	Visibility in days
9121	2-Mar-2010	10-Apr-2010	39
21385	28-Feb-2011	2-Mar-2011	2
24523	25-Nov-2011	16-Dec-2011	21
24953	5-Jul-2013	31-Jul-2013	26
25933	26-Jun-2015	29-Jun-2015	3
27969	15-Sep-2013	6-Feb-2015	509
33849	28-Jun-2010	3-Aug-2010	36
35631	2-Apr-2015	9-Apr-2015	7
37162	16-Jul-2014	8-Nov-2014	115
37371	29-Jan-2013	11-Apr-2014	437
38077	17-May-2010	25-May-2010	8
38761	22-Sep-2010	22-Oct-2010	30
41599	7-Jan-2010	30-Mar-2010	82
51002	27-Jul-2010	29-Jul-2010	2
53053	15-Apr-2015	27-May-2015	42

November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Route leak visibility (in days)



November 10th, 2015 - Anurag Bhatia - Hurricane Electric - bdNOG 4 - Sreemongal, Bangladesh - Misused Top ASNs

Longest leak

1445 days (~3.9 years) for AS1 by AS23383

Sample AS_PATHs

186.65.112.0/20,30132 6939 23520 23383 1 65430

186.65.112.0/20,8283 5580 23520 23383 1

190.185.108.0/22,30132 6939 23520 23383 1 65430

190.185.108.0/22,8283 5580 23520 23383 1

Most amusing AS_PATH ever!

31019 39326 39326 3356 7029 1614 1614 1614 1614 **1 2 3 4 5**

TABLE_DUMP_V2|02/02/14

00:00:01|A|195.69.146.99|50763|74.122.136.0/24|50763 8943 3549 7029 1614
1614 1614 1614 1 2 3 4 5|IGP

References

1. RIPE RIS Raw data - <https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data>
2. bgpdump tool - <http://www.ris.ripe.net/source/bgpdump/>
3. HE's BGP toolkit - <http://bgp.he.net>

Thankyou!

Questions?

Peering?

Transit requirement?

anurag@he.net

<http://he.net>

<http://as6939.peeringdb.com>