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

How they are “misused” ?

Reasons for mis-use...

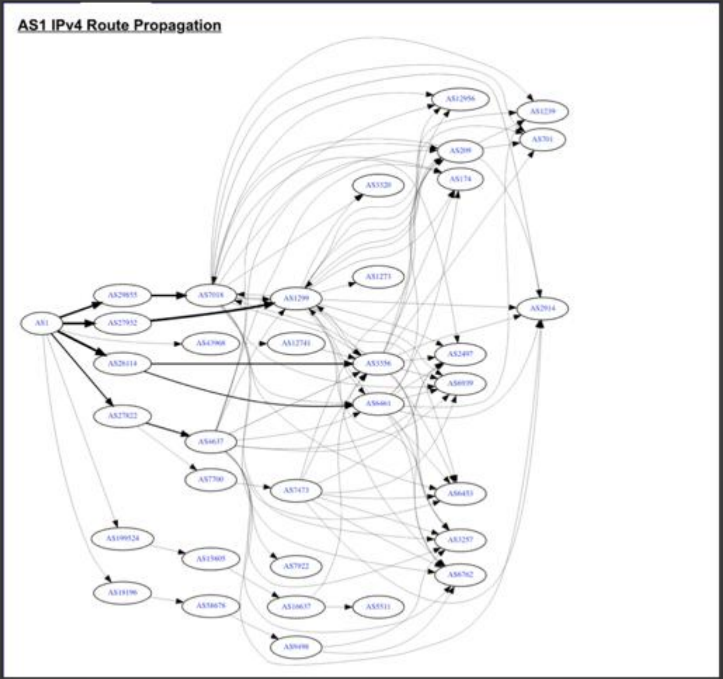
- “Copy-paste” of sample prepend configuration “1 2 3”
- Mistakenly typing “1 2 or 3” in prepend rules in route filter / export policy statement

Impact of mis-use

Hard to determine statistically but ...

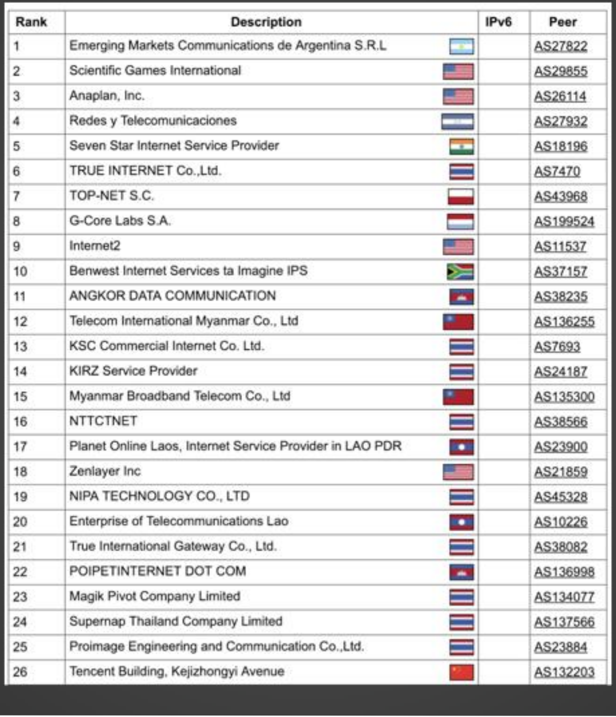
- Shows unexpected relationship of leaking AS with top ASN and among top ASNs!
- Considered to be “AS hijack” and bad for trust based BGP routing
- Can result in *(a wrongly prepended)* announcement getting filtered across parts of internet
- Chances of broken connectivity of these routes with top ASNs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

AS1 Graph V4



AS1 IPv4 Route Propagation

AS1 Peer V4



Rank	Description	IPv6	Peer
1	Emerging Markets Communications de Argentina S.R.L		AS27822
2	Scientific Games International		AS29855
3	Anaplan, Inc.		AS26114
4	Redes y Telecomunicaciones		AS27932
5	Seven Star Internet Service Provider		AS18196
6	TRUE INTERNET Co.,Ltd.		AS7470
7	TOP-NET S.C.		AS43968
8	G-Core Labs S.A.		AS199524
9	Internet2		AS11537
10	Benwest Internet Services ta Imagine IPS		AS37157
11	ANGKOR DATA COMMUNICATION		AS38235
12	Telecom International Myanmar Co., Ltd		AS136255
13	KSC Commercial Internet Co. Ltd.		AS7693
14	KIRZ Service Provider		AS24187
15	Myanmar Broadband Telecom Co., Ltd		AS135300
16	NTTCTNET		AS38566
17	Planet Online Laos, Internet Service Provider in LAO PDR		AS23900
18	Zenlayer Inc		AS21859
19	NIPA TECHNOLOGY CO., LTD		AS45328
20	Enterprise of Telecommunications Lao		AS10226
21	True International Gateway Co., Ltd.		AS38082
22	POIPETINTERNET DOT COM		AS136998
23	Magik Pivot Company Limited		AS134077
24	Supernap Thailand Company Limited		AS137566
25	Proimage Engineering and Communication Co.,Ltd.		AS23884
26	Tencent Building, Kejizhongyi Avenue		AS132203

Hunting for leakers...

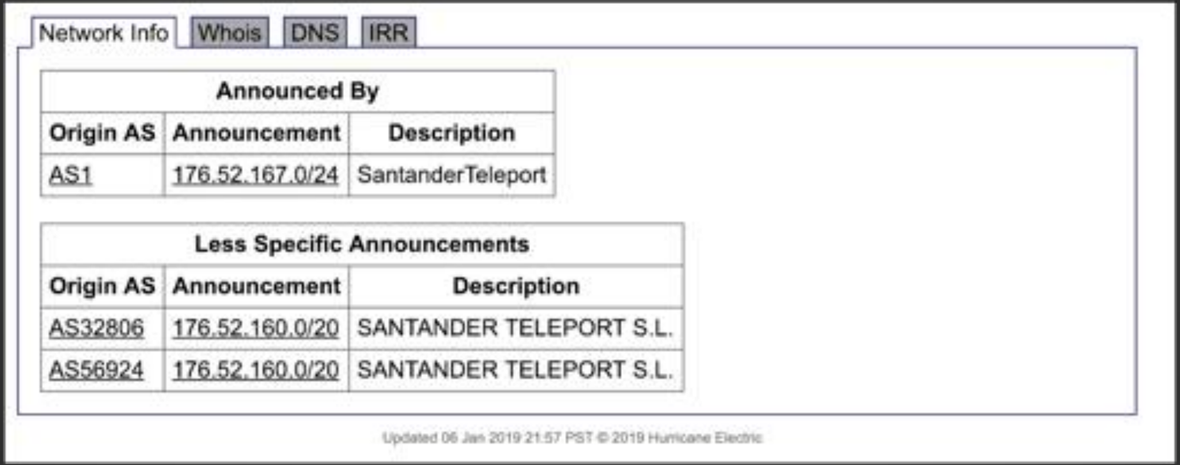
- Analysis of routing table from multiple RIPE RIS collectors and Oregon Route-views
- Analysis from Jan 2015 to Dec 2018
- Looking for cases where top 3 ASNs appear in AS_PATH for routes which belong to other ASNs.
- Focus of top ASNs appearance with prepends in the routing table
- Leaks which appeared for less than 24hrs are not collected

Leak or legitimate?

Logic used to detect leak:

- ASN in the AS_PATH is unrelated entity and is not a ASN owned by top 3 ASNs
- Prefix appearing to be originating from top ASN happens to be allocated to ASN on the left side of the leaked ASN in the as_path
- Prefix appearing to be originated from top ASN has a less specific origination by ASN on the left side of the leaked ASN in the as_path

Leak or legitimate - An example



Announced By		
Origin AS	**Announcement**	**Description**
AS1	176.52.167.0/24	SantanderTeleport

Less Specific Announcements		
Origin AS	**Announcement**	**Description**
AS32806	176.52.160.0/20	SANTANDER TELEPORT S.L.
AS56924	176.52.160.0/20	SANTANDER TELEPORT S.L.

Updated 06 Jan 2019 21:57 PST © 2019 Hurricane Electric

Some of who leaked AS1...

AS Number	Start Date	End Date	Days
26114	2015-01-01	2018-12-31	1460
13227	2015-01-01	2018-12-27	1456
27822	2017-04-17	2018-12-31	623
133498	2015-01-01	2016-08-31	608
199524	2017-09-16	2018-12-31	471
27932	2017-10-31	2018-12-31	426
18196	2017-12-14	2018-12-31	382
48085	2017-11-13	2018-11-21	373
43968	2018-01-14	2018-12-31	351
37157	2018-03-27	2018-12-31	279

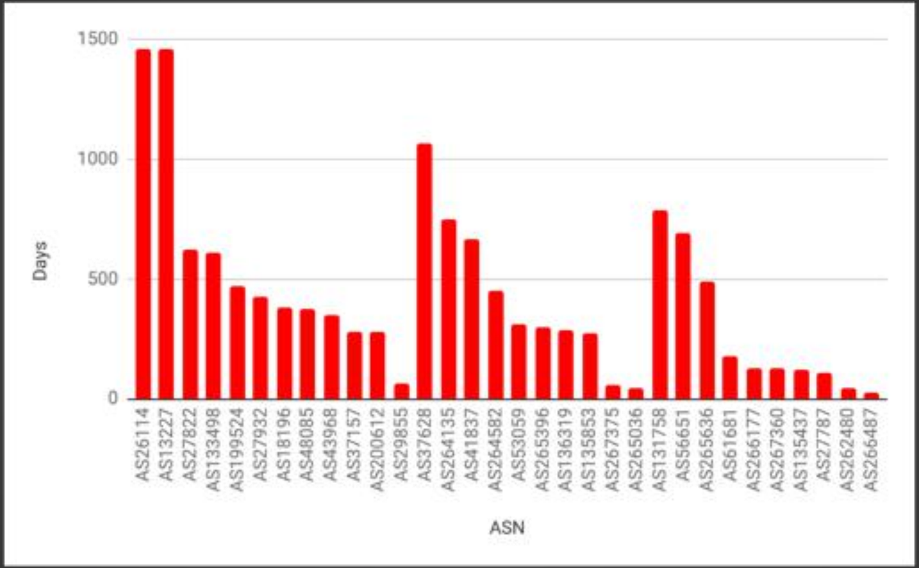
Some of who leaked AS2...

AS Number	Start Date	End Date	Days
37628	2016-02-02	2018-12-31	1063
264135	2016-12-15	2018-12-31	746
41837	2017-03-02	2018-12-31	669
264582	2017-07-19	2018-10-10	448
53059	2017-12-29	2018-11-05	311
265396	2018-03-10	2018-12-31	296
136319	2018-03-20	2018-12-31	286
135853	2018-04-03	2018-12-31	272
267375	2018-11-06	2018-12-31	55
265036	2018-11-14	2018-12-31	47

Some of who leaked AS3...

AS Number	Start Date	End Date	Days
131758	2016-11-03	2018-12-31	788
56651	2017-02-05	2018-12-31	694
265636	2017-08-31	2018-12-31	487
61681	2018-07-09	2018-12-31	175
266177	2018-08-25	2018-12-31	128
267360	2018-08-27	2018-12-31	126
135437	2018-09-04	2018-12-31	118
27787	2018-09-11	2018-12-31	111
262480	2018-11-19	2018-12-31	42
266487	2018-12-04	2018-12-31	27

Route leak visibility (in days)



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
```

Preventing such leaks

- If prepending is needed, prepend correctly i.e by repeating your own ASN multiple times
- Avoid typing ASNs by hand in config and prefer to copy paste *(helps for long ASNs)*
- Lookout for your router’s vendor's documentation on how to prepend
- Use tools like bgpq3 to generate filters for your neighbors
- Filter not only based on prefix but as ASN/AS_Path as well!
- IX’es can use tools like arouteserver to generate route server config with filtering
- Encourage and use RPKI!

Prepend Sample Config - Cisco IPv4

Create route-map which would be applied in OUT direction with specific peer

```
route-map NetworkA-OUT permit 10
 set as-path prepend 64520 64520   <--- Important to prepend your own ASN. Don't use any other random number here!
```

Call the route-map in out direction on the BGP session for IPv4

```
router bgp 64520
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 64521
 neighbor 192.168.1.2 route-map NetworkA-OUT out
 neighbor 192.168.1.2 route-map NetworkA-IN in
 no auto-summary
```

Prepend Sample Config - Cisco IPv6

Create route-map which would be applied in OUT direction with specific peer

```
route-map NetworkA-OUT permit 10
 set as-path prepend 64520 64520   <--- Important to prepend your own ASN. Don’t use any other random number here!
```

Call the route-map in out direction on the BGP session for IPv6

```
 !
 address-family ipv6
 neighbor 2001:DB8:1:1::2 activate
 neighbor 2001:DB8:1:1::2 route-map NetworkA-OUT out
 network 2001:DB8:2::/48
 exit-address-family
!
```

Prepend Sample Config - JunOS

Create export policy which would be applied to the peer

```
edit policy-options policy-statement Network-A-Out
set term a from prefix-list Pool-set1
set term a then as-path-prepend “64520 64520” <--- Important to prepend your own ASN. Don’t use any other random number here!
```

Call the route-map in out direction on the BGP session

```
set protocols bgp group transits neighbor  192.168.1.2 export Network-A-Out
```

Reference

1. Oregon Route Views

2. RIPE RIS - http://www.ripe.net/data-tools/stats/ris/routing-information-service

3. Hurricane Electric BGP toolkit - bgp.he.net

4. Bgpdump tool - https://bitbucket.org/ripencc/bgpdump/wiki/Home

Thankyou!

Questions?
Peering?

Twitter: @anurag_bhatia

anurag@he.net

AS6939

http://he.net

http://as6939.peeringdb.com