Everybody Leaks

Alexander Azimov

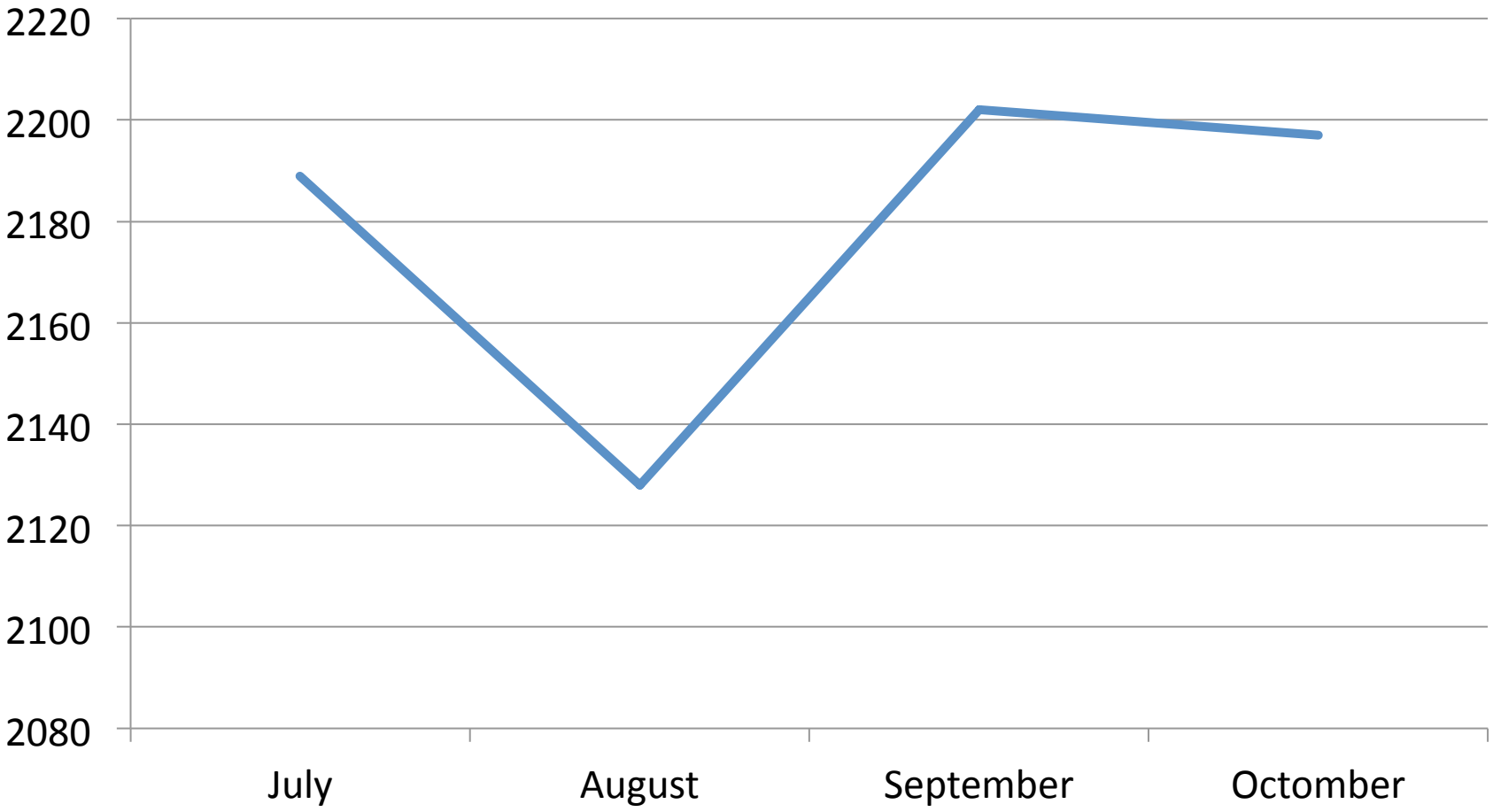
Route Leaks

Abnormal subpath:

1. Provider -> Customer -> Provider
2. Provider -> Customer -> Peering
3. Peering -> Customer -> Provider
4. Peering -> Peering -> Peering

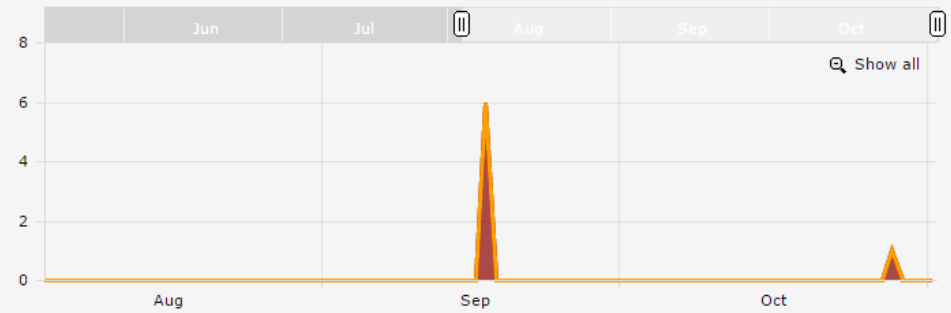
Amount?

New Abnormal Paths Monthly



There problem is far away…

AS3333 (RIPE-NCC-AS) ROUTE LEAKS



Leaked Prefixes
Leaked Paths

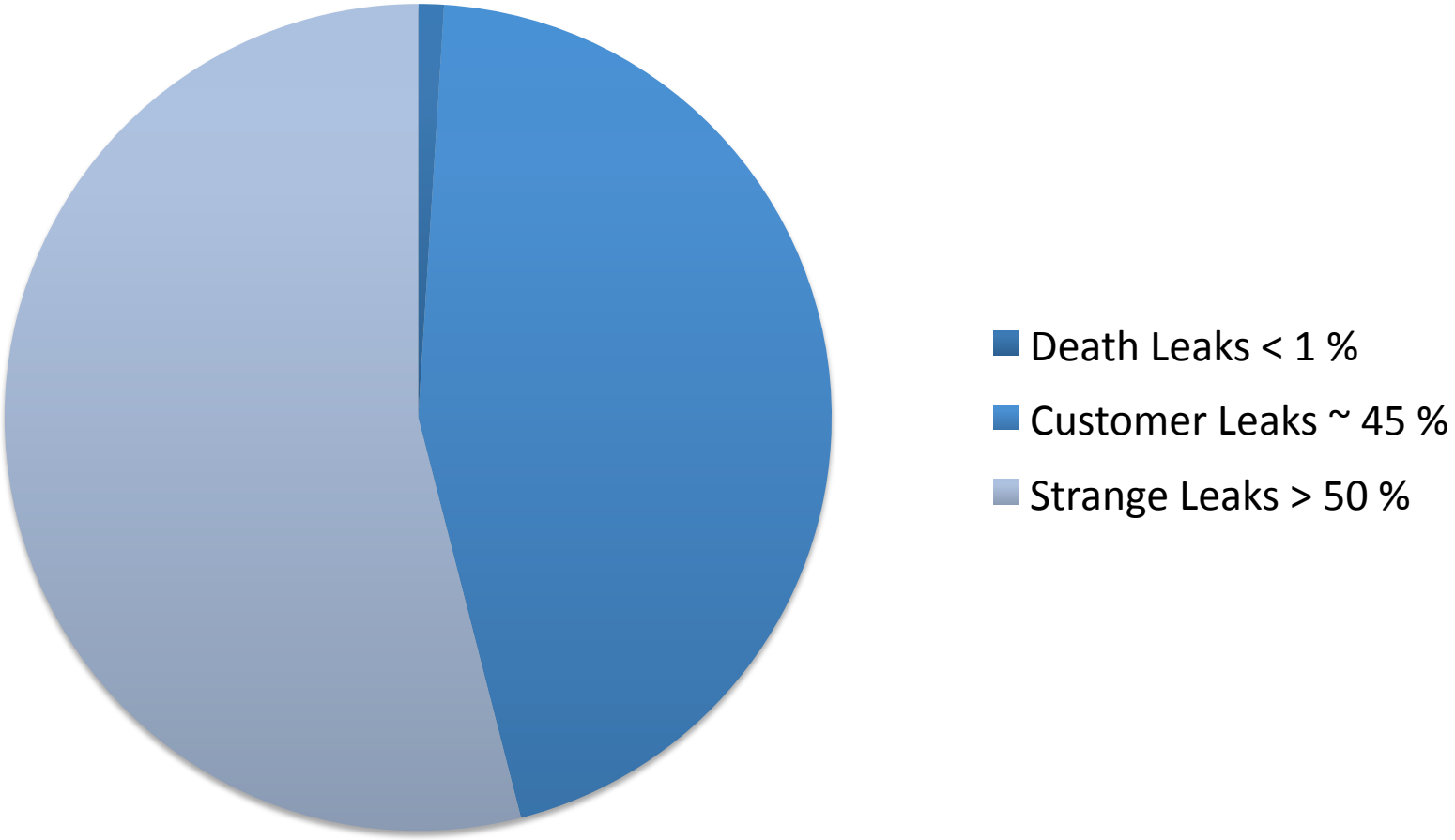
August 4, 2014 - November 2, 2014

Route leaks occur when AS announces provider's or peering's prefixes to other providers or peerings. This results in increase of delays or traffic drop for leaked prefixes and could exhaust traffic bandwidth of a "leaker" AS.

Leaked Prefixes (0) | Leaked Paths (0)

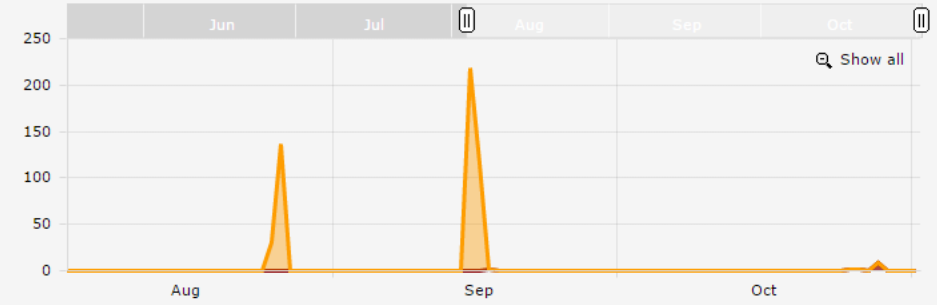
	Origin	Prefix	Abnormal Path	First seen	Last seen	
1	AS3333	193.0.0.0/21	12872 **39056** 35320	2014-10-29 07:16:00	2014-10-29 07:16:00	Archive
2	AS3333	193.0.18.0/23	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive
3	AS3333	193.0.12.0/23	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive
4	AS3333	193.0.20.0/23	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive
5	AS3333	193.0.10.0/23	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive
6	AS3333	193.0.22.0/23	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive
7	AS3333	193.0.0.0/21	174 **46664** 5580	2014-09-18 11:02:00	2014-09-18 11:02:00	Archive

Leak Distribution



Strange leaks are very strange

AS49345 (Continental_Group-AS) ROUTE LEAKS



Leaked Prefixes
Leaked Paths

August 4, 2014 - November 2, 2014

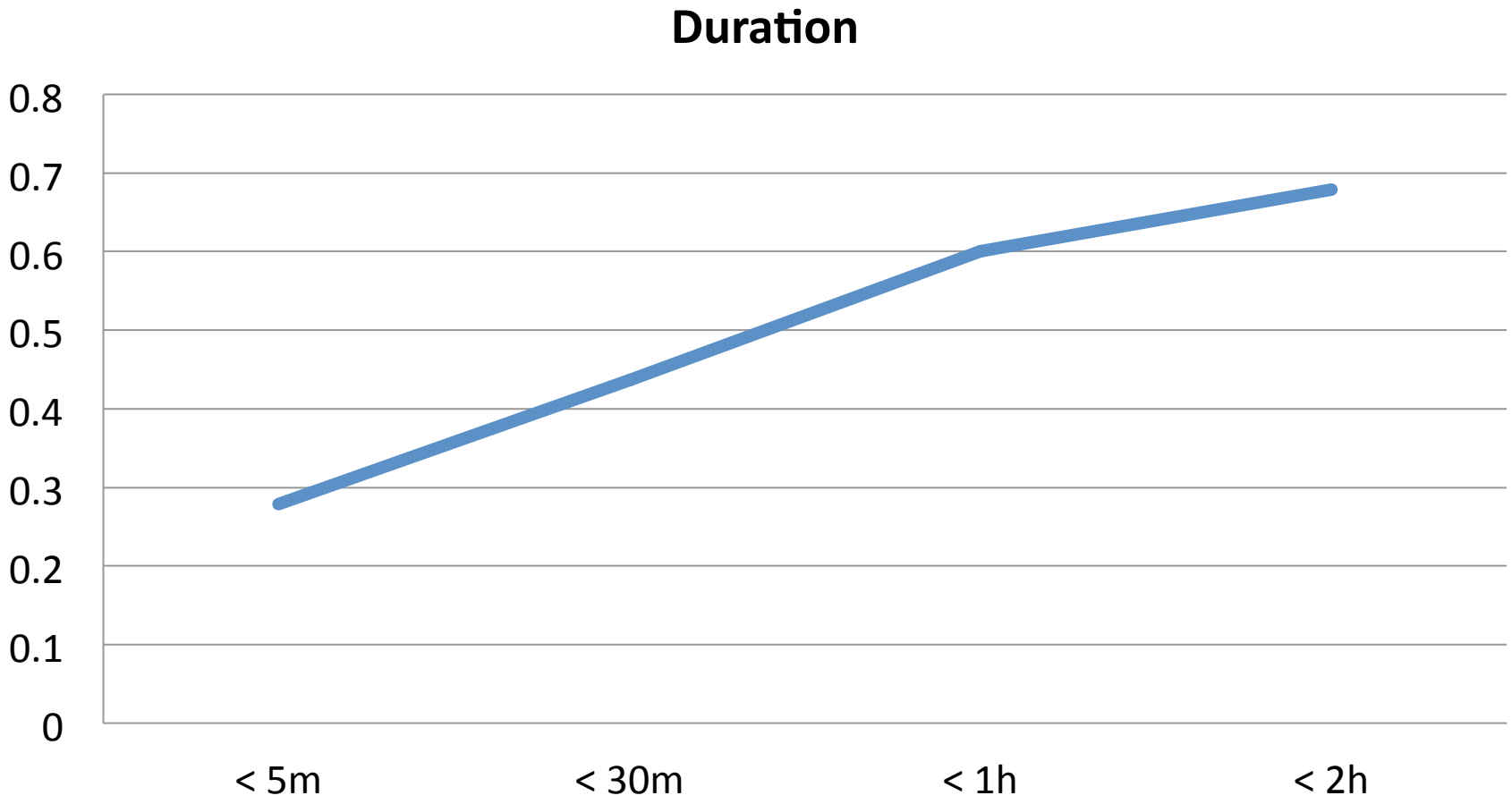
Route leaks occur when AS announces provider's or peering's prefixes to other providers or peerings. This results in increase of delays or traffic drop for leaked prefixes and could exhaust traffic bandwidth of a "leaker" AS.

Leaked Prefixes (0) | Leaked Paths (0)

	Origin	Prefix	Abnormal Path	First seen	Last seen	
1	AS15169	74.125.225.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
2	AS15169	74.125.72.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
3	AS15169	74.125.28.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
4	AS15169	74.125.202.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
5	AS15169	74.125.238.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
6	AS15169	74.125.20.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
7	AS15169	173.194.125.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
8	AS15169	74.125.69.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
9	AS15169	1.0.0.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive
10	AS15169	66.249.72.0/24	44843 **49345** 31500	2014-09-16 16:06:00	2014-09-17 12:38:00	Archive

Target Leak of Google's prefixes

Route Leak Dynamics



30% of leaks are long-term and unnoticed!

What could be done?

1. Outbound prefix filtering;
2. Inbound prefix filtering or prefix limit;
3. Collaboration, more collaboration!
4. Announce isn’t end of story, you need to monitor it;

Monitoring announces

- Raw data

RIPE & Routeviews – thank you!

- Renesys
- BGPMon
- Radar by Qrator

Questions?

radar.qrator.net