Detecting Routing Incidents

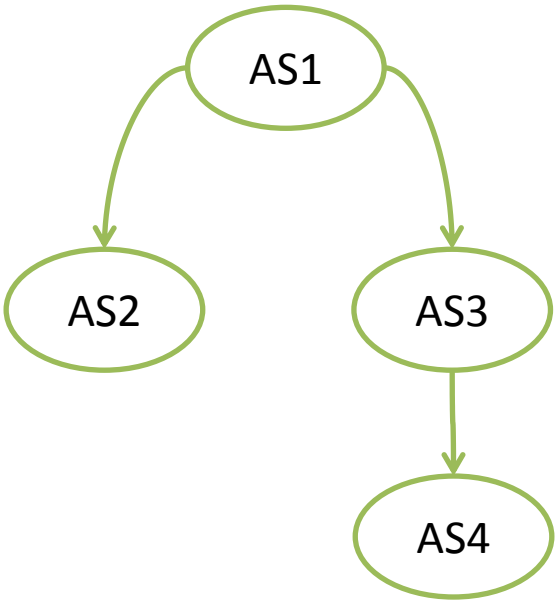
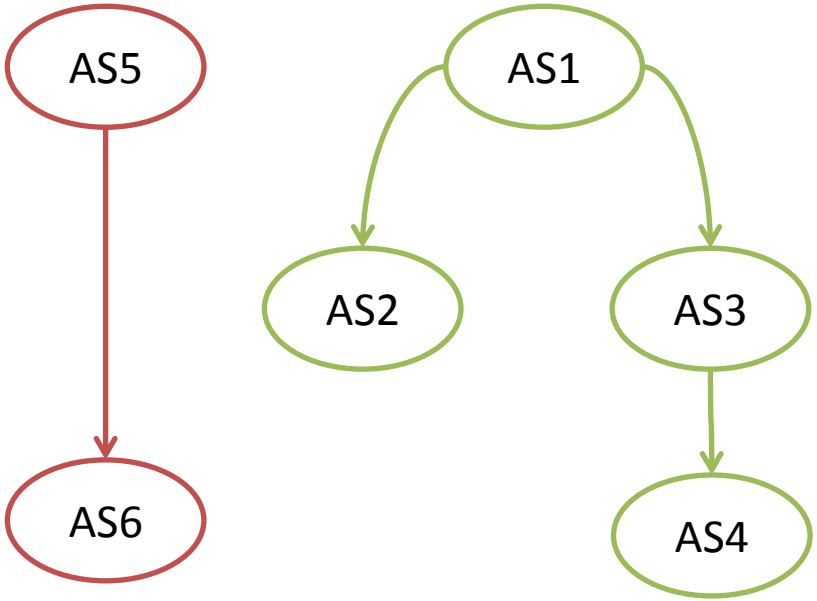
Alexander Azimov
Qrator Labs

Routing Incidents

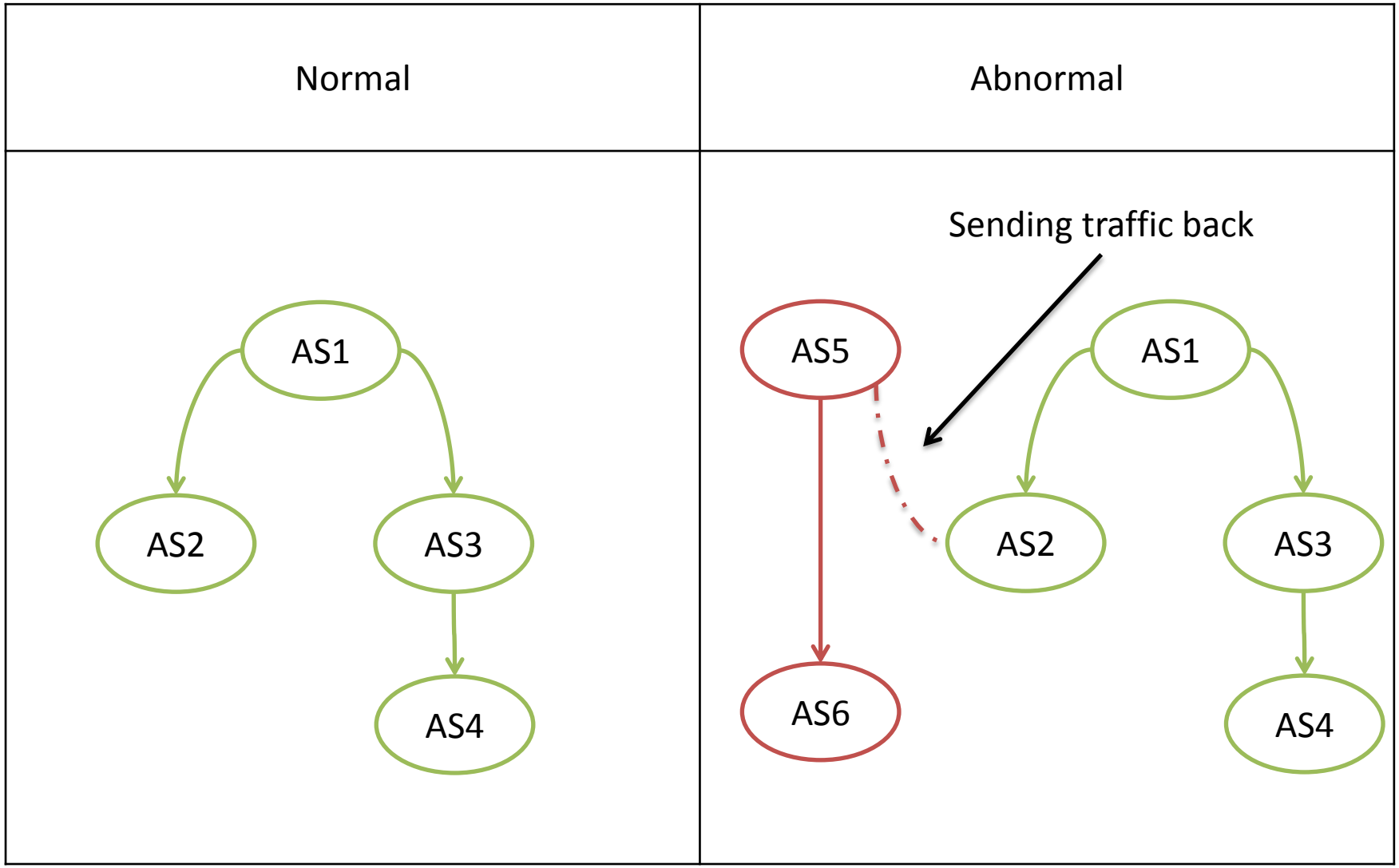
1. Google – 2007: Hijack
2. YouTube – 2008: Hijack
3. AS27664 – 2008: Death Leak (First one?)
4. AS23724 – 2010: Global Hijack

And thousands of other less famous incidents

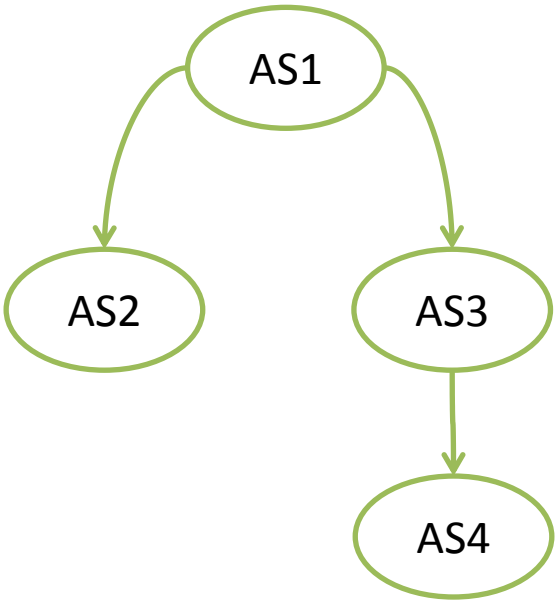
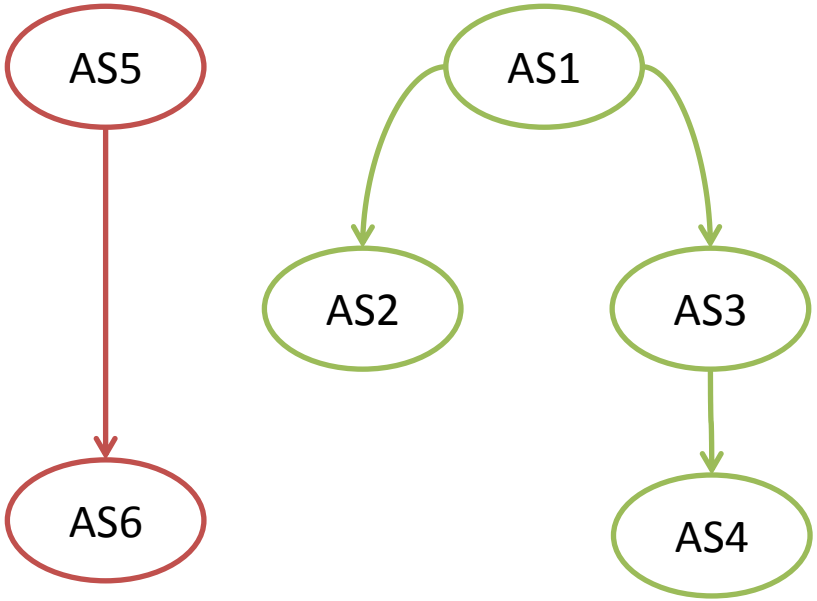
Prefix Hijacking: DoS

Normal	Abnormal
	

Prefix Hijacking: Man-in-the-middle

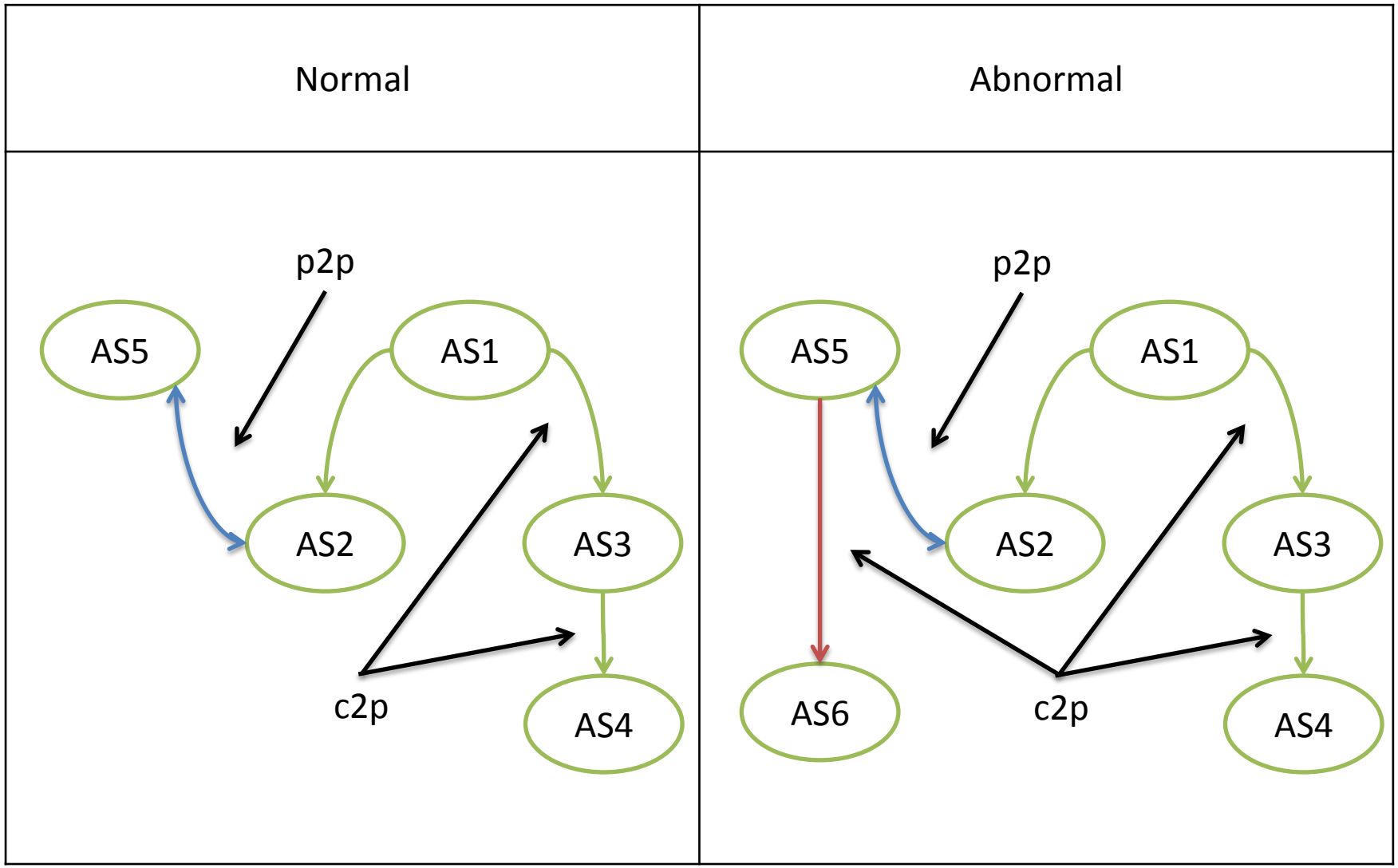


Prefix Hijacking + AS Path hiding

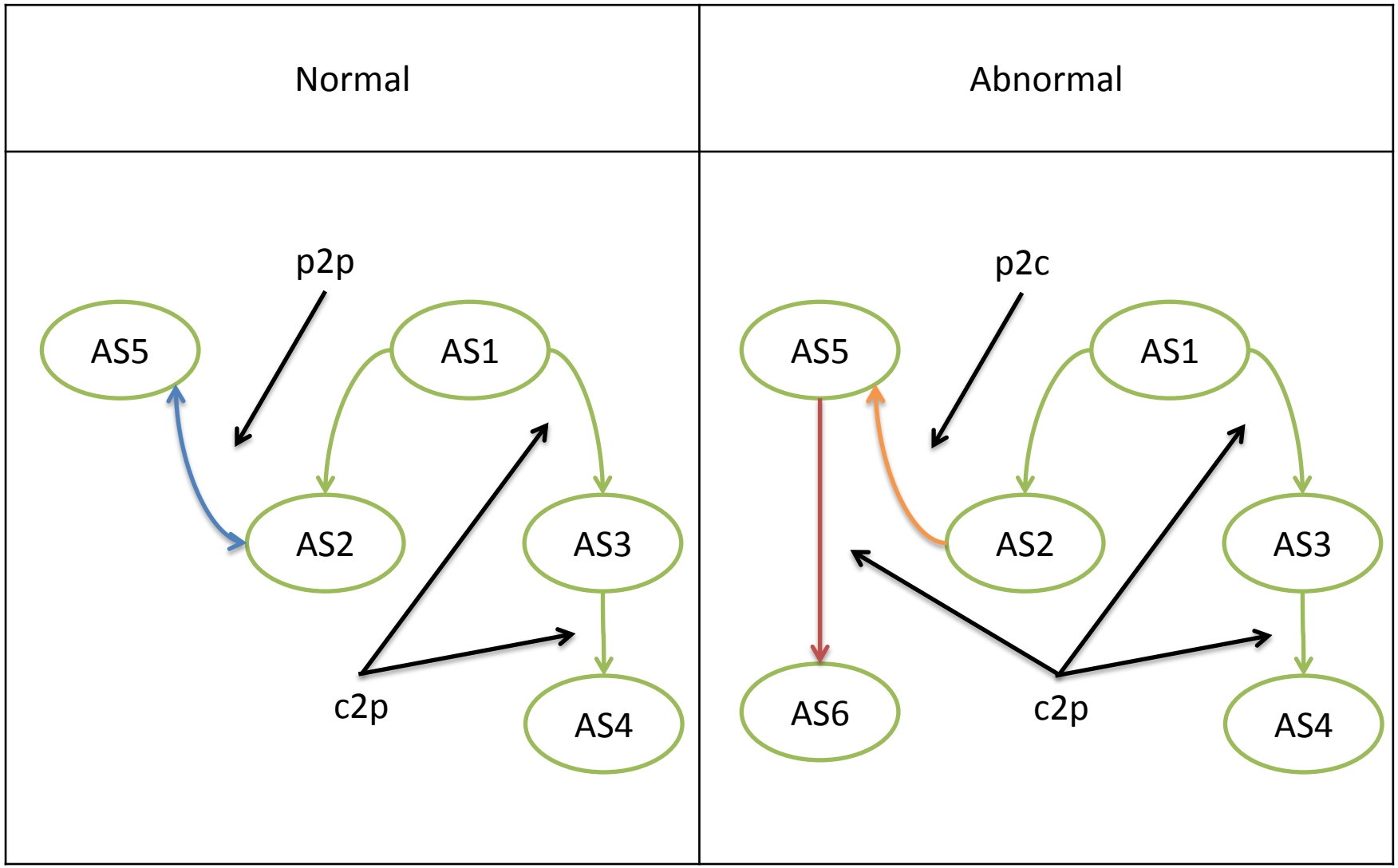
Normal	Abnormal
	Prepend 1, 2 

RPKI doesn't help

Route Leak


Normal
Abnormal
p2p
AS5
AS1
AS2
AS3
c2p
AS4
p2p
AS5
AS1
AS2
AS3
AS6
c2p
AS4

Death Leak


Normal
Abnormal
p2p
AS5
AS1
AS2
AS3
c2p
AS4
p2c
AS5
AS1
AS2
AS3
AS6
c2p
AS4

Routing incidents

- Is there any opportunity to automatically mitigate routing incidents?

No

- Could origin AS detect the problem?

No

- Is there any opportunity to detect routing incidents?

Yes, because AS Path is abnormal in all cases

Abnormal Paths

AS2 is new provider for AS1	
AS2 is customer for AS1	AS3 is provider for AS2
AS2 is customer for AS1	AS3 is peering for AS2
AS2 is peering for AS1	AS3 is provider for AS2
AS2 is peering for AS1	AS3 is peering for AS2

Death Leak

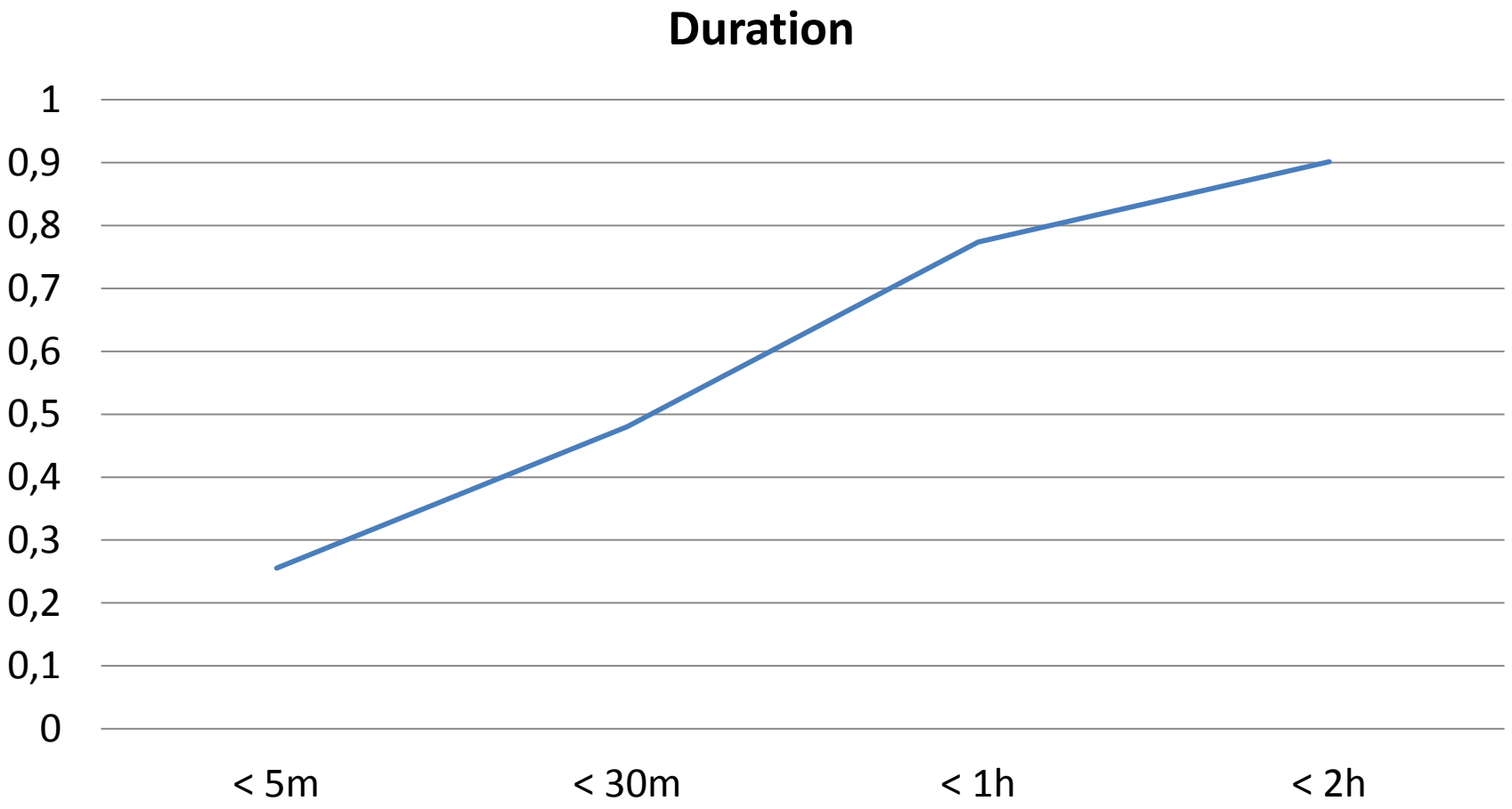
The Main Reason

The Main Reason

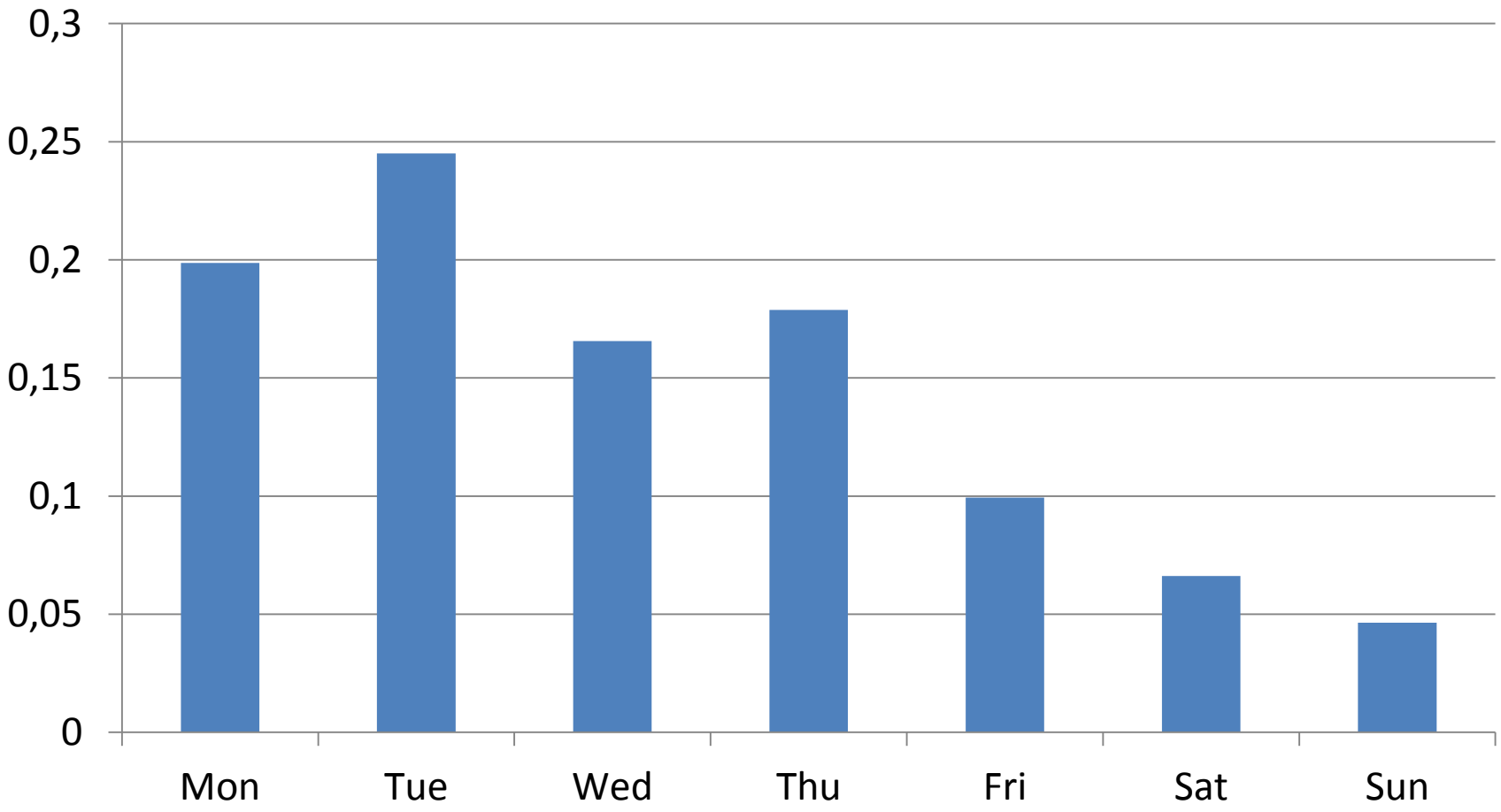
Last Week Death Leaks

Leaker	Abnormal Path	Duration	Country
AS47579	20485 47579 8359	20 min	RU
AS32421	3257 32421 2914	5 min	US
AS45250	4134 45250 9304	5 min	TW
AS12810	48159 12810 9498	15 min	IQ
AS48159	27757 26613 1239	6 h	EC

Route Leak Dynamics

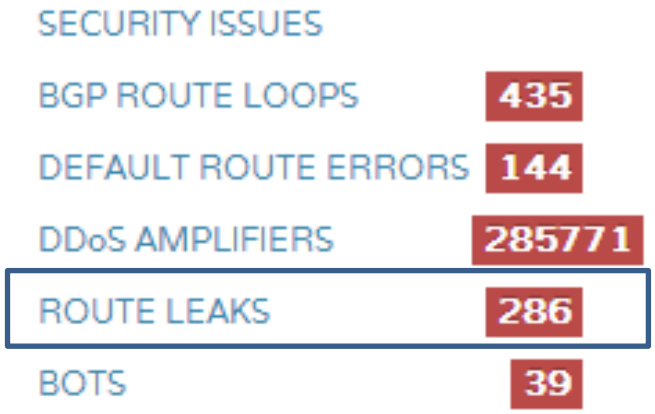


Weekly periods



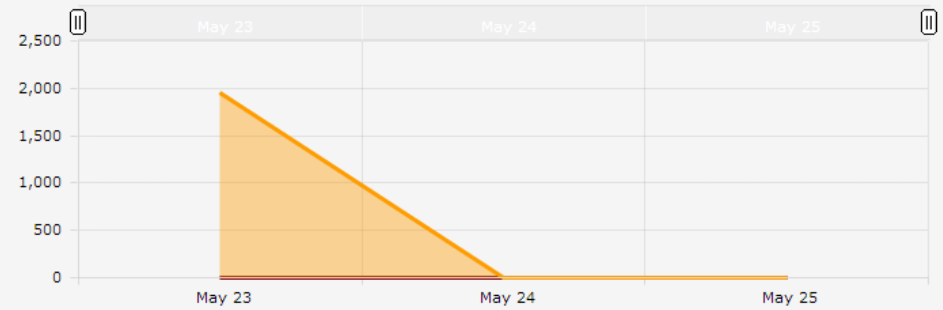
Holidays!

Radar by Qrator



Radar by Qrator

AS47579 (Pilot) ROUTE LEAKS



Leaked Prefixes
Leaked Paths

May 23, 2014 - May 25, 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	AS48287	193.232.158.0/23	20485 **47579** 8359	2014-05-23 15:51:00	2014-05-23 16:11:00	Archive
2	AS48287	193.232.144.0/22	20485 **47579** 8359	2014-05-23 15:51:00	2014-05-23 16:11:00	Archive
3	AS10029	180.151.7.0/24	20485 **47579** 8359	2014-05-23 15:51:00	2014-05-23 16:11:00	Archive
4	AS28033	200.7.14.0/24	20485 **47579** 8359	2014-05-23 15:51:00	2014-05-23 16:11:00	Archive
5	AS48287	109.70.24.0/21	20485 **47579** 8359	2014-05-23 15:51:00	2014-05-23 16:11:00	Archive

AS48287

20485 **47579** 8359

Which is the worst case?

1. Prefix Hijacking?
2. Man in the middle?
3. Route Leaks?

Which is the worst case?

1. Prefix Hijacking?
2. Man in the middle?
3. Route Leaks?

They are all the worst case.

Prefix announce isn’t the end of the story.

Take care of your prefixes’ paths.

Questions?

radar.qrator.net