

AS-Path Analysis

Testing Claims of “Tier 1” Status and Examining BGP Routing Anomalies

Version 1.1

August, 2006

Vijay Kumar Adhikari

Gaurab Raj Upadhaya, Bill Woodcock

Packet Clearing House

Background

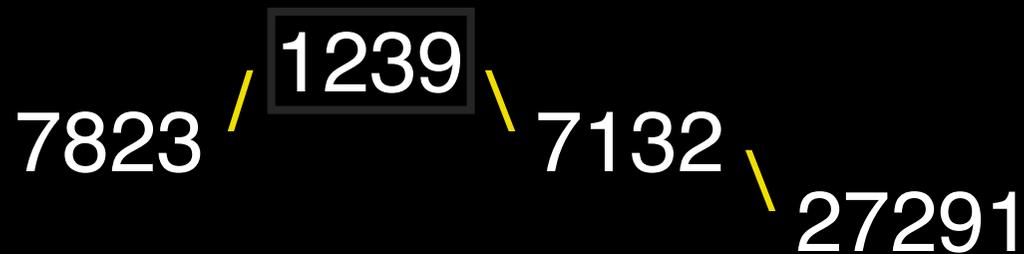
Autonomous systems which claim “tier-1” status differentiate themselves from others by claiming that they do not receive transit from any other autonomous system.

Background

Autonomous systems which do not receive transit may reach other ASes by selling transit to them or by peering with them.

Background

All AS-paths take one of two forms:
One in which the “center” is an AS which provides transit to two down-stream ASes:



Dupont **buys** Sprint **sells** SBC **sells** Fry's

Background

All AS-paths take one of two forms:
Or one in which the “center” is a peering session between two ASes, each of which provides transit to one downstream AS:



PCH **buys** Verio **peers** Sprint **sells** SBC **sells** Fry's

Proposition

Since there can exist no more than one peering session in any AS-path,

No more than two ASNs can make a legitimate claim to “tier-1” status with respect to any valid AS-path.

Seed-list to test

For an arbitrary starting-point to test our proposition, we took the intersection of the lists of most commonly-occurring transit ASes from a number of routers:

701	UUNet / MCI	1239	Sprint
3356	Level 3	2914	NTT / Verio
7018	AT&T	6461	MFN
209	Qwest	2828	XO Communications
3549	Global Crossing	4637	Reach

Testing the Proposition

We find anomalous cases, in which three or more ASNs from our test list occur in the same AS-path:

65.215.36.0/24

3549

Global
Crossing

6221

Cybersites

3356

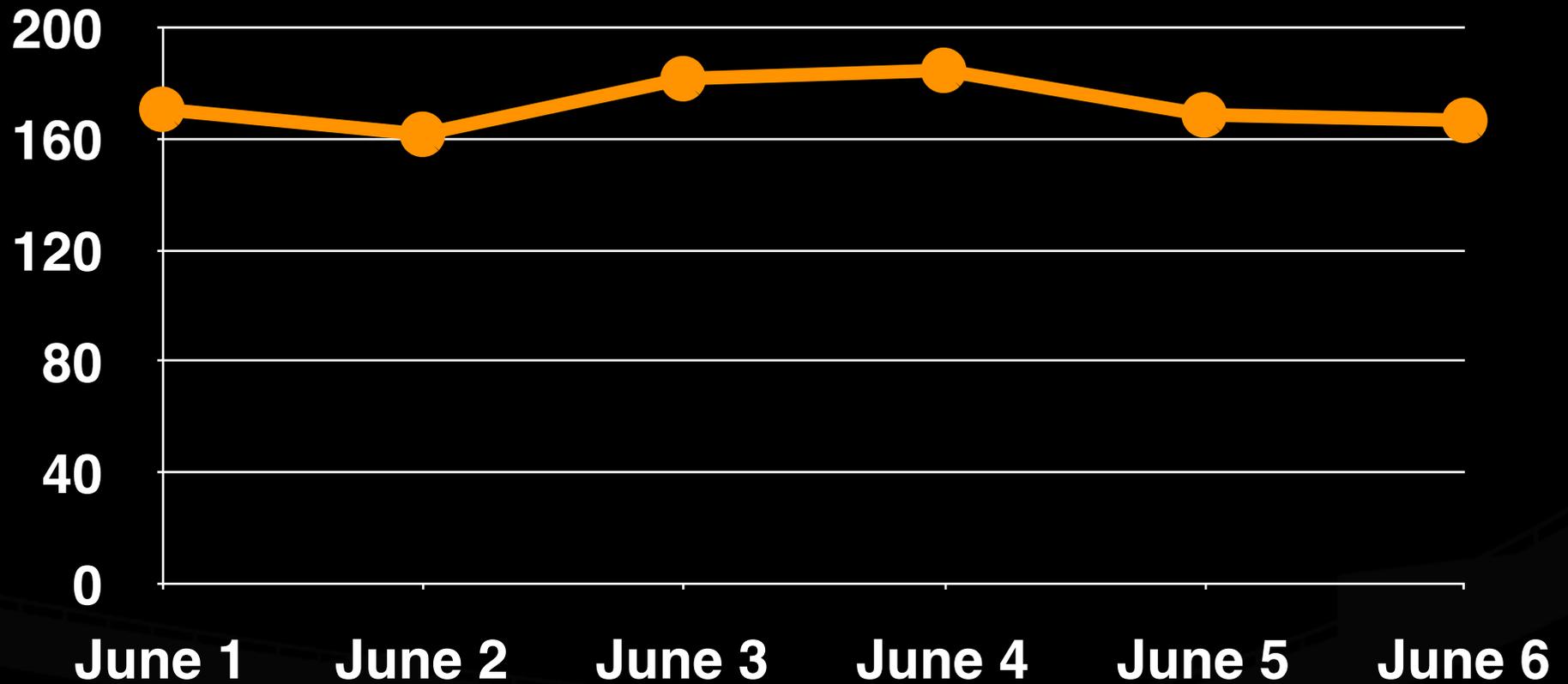
Level 3

701

UUNET

22907

Leaked Routes (more than 2 Tier1 ASNs)



More Anomalies

Inconsistent ASNs

Non-contiguous Repeats

Private ASNs

Unallocated ASNs

Inconsistent Prefix Announcements

Examples

12.33.218.0/24

Announced by more than 1 ASNs:

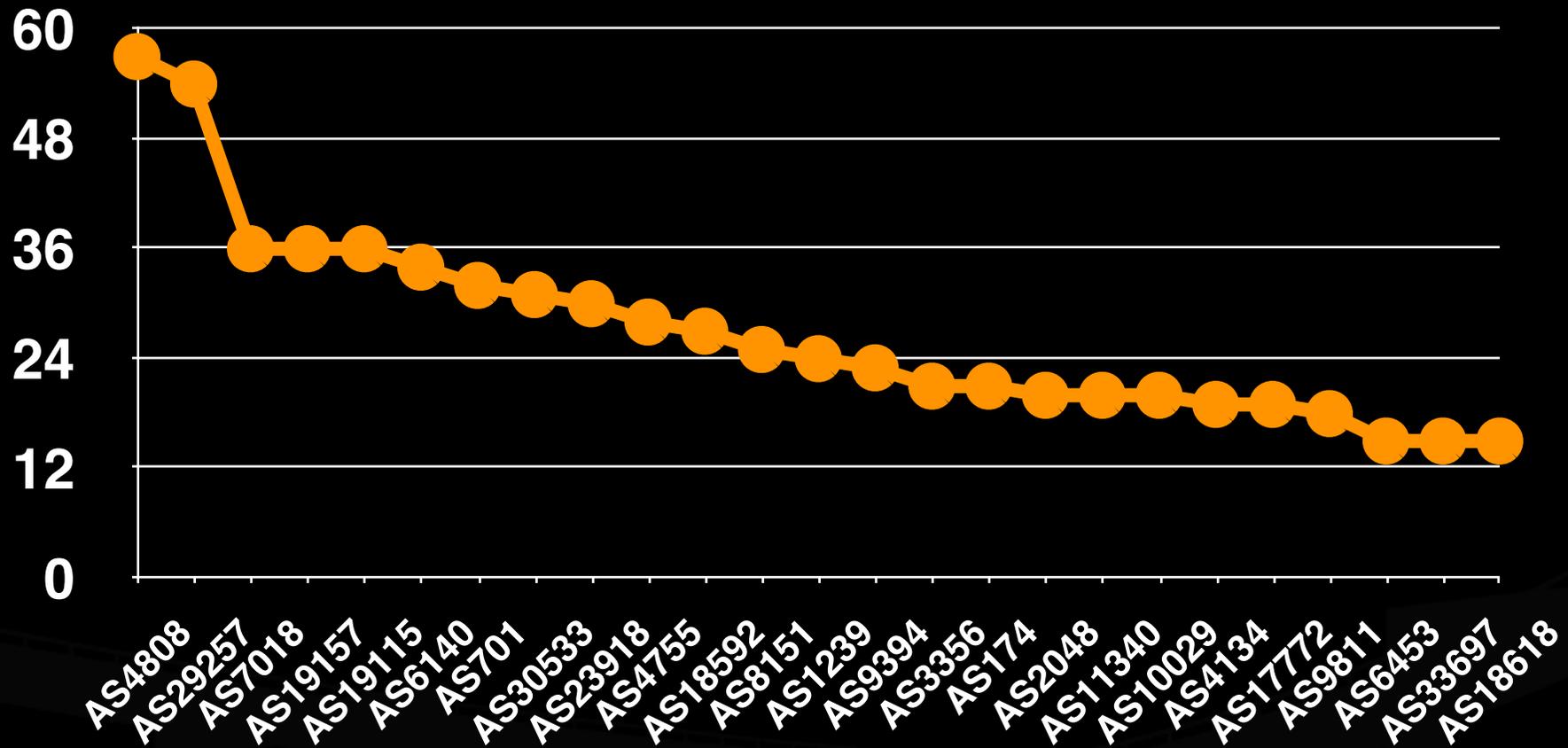
22057, 23181

12.64.255.0/24

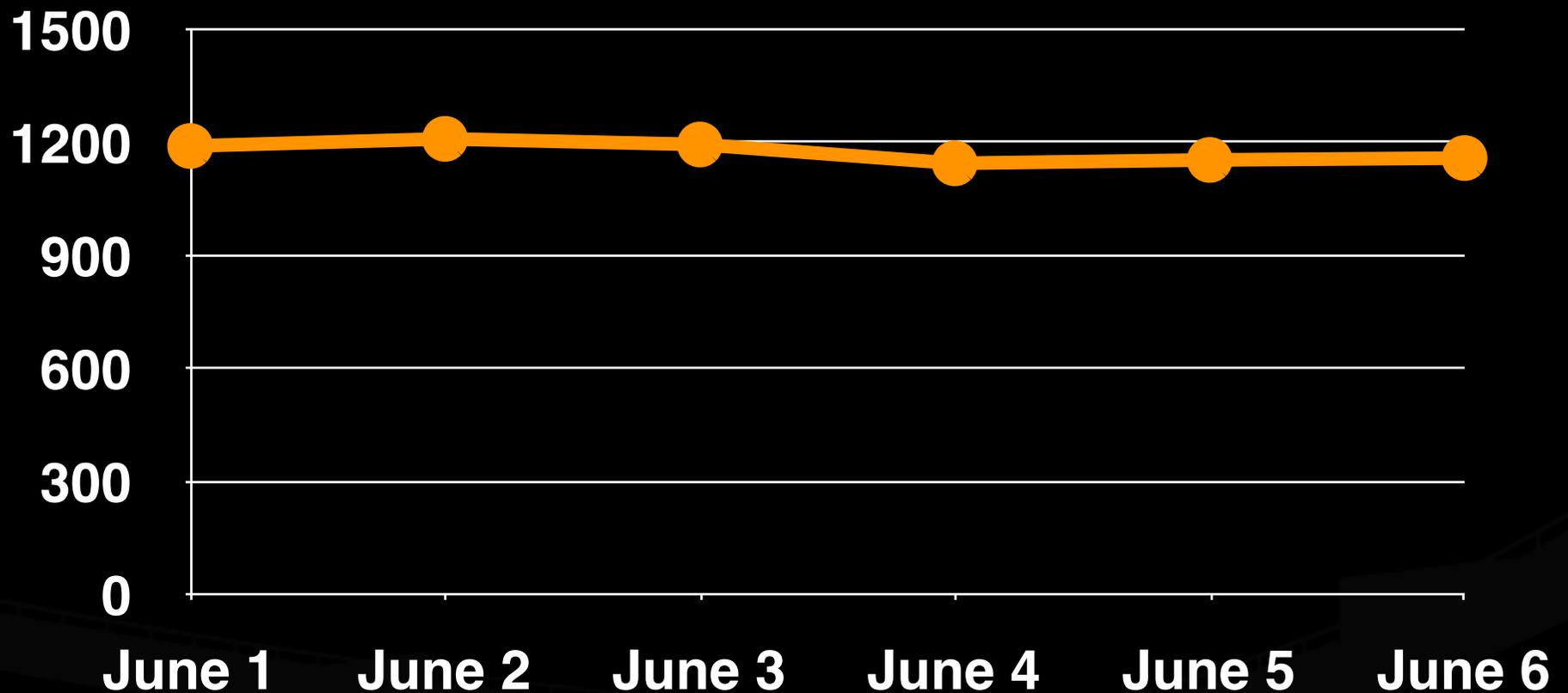
Announced by more than 1 ASNs:

4264, 17228, 17229, 17233

Inconsistent Prefix Announcements



Inconsistent Prefix Announcements

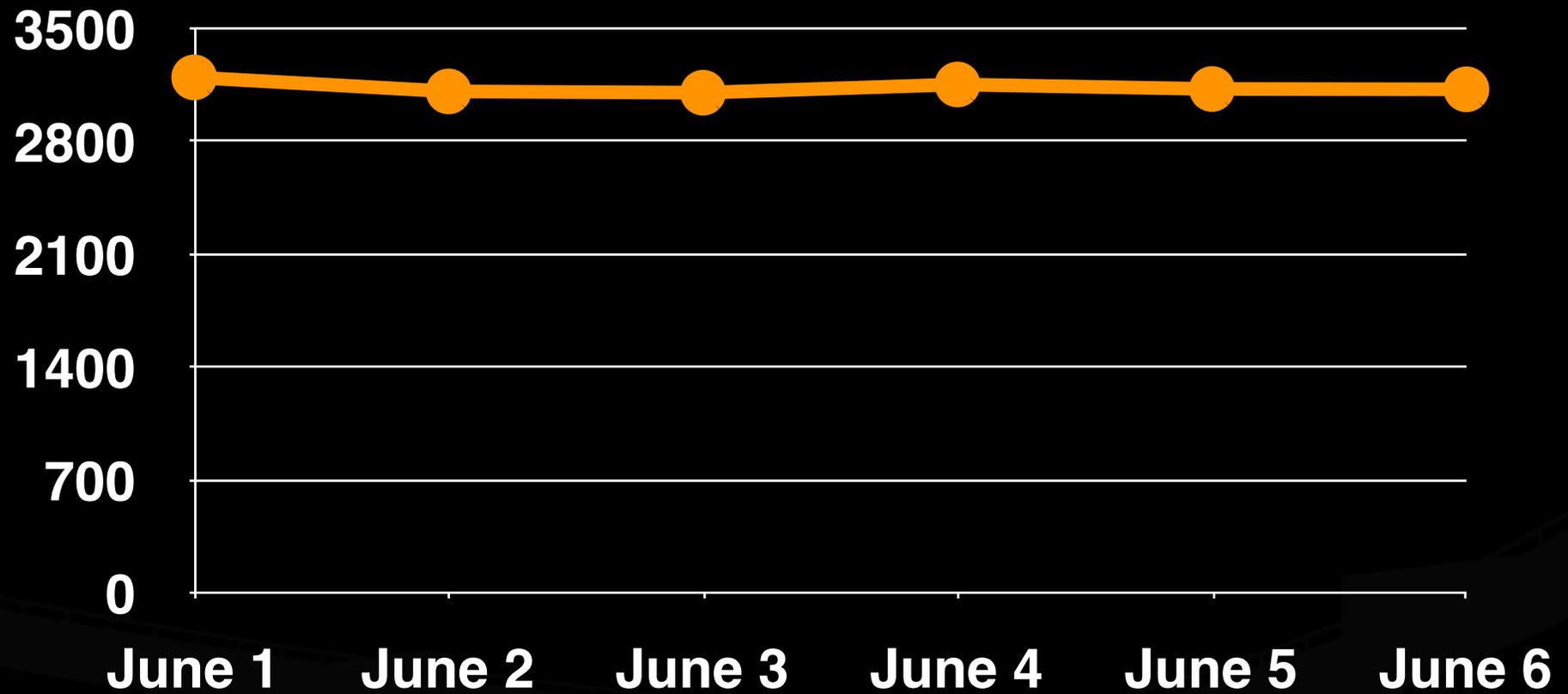


Non-contiguous Repeats

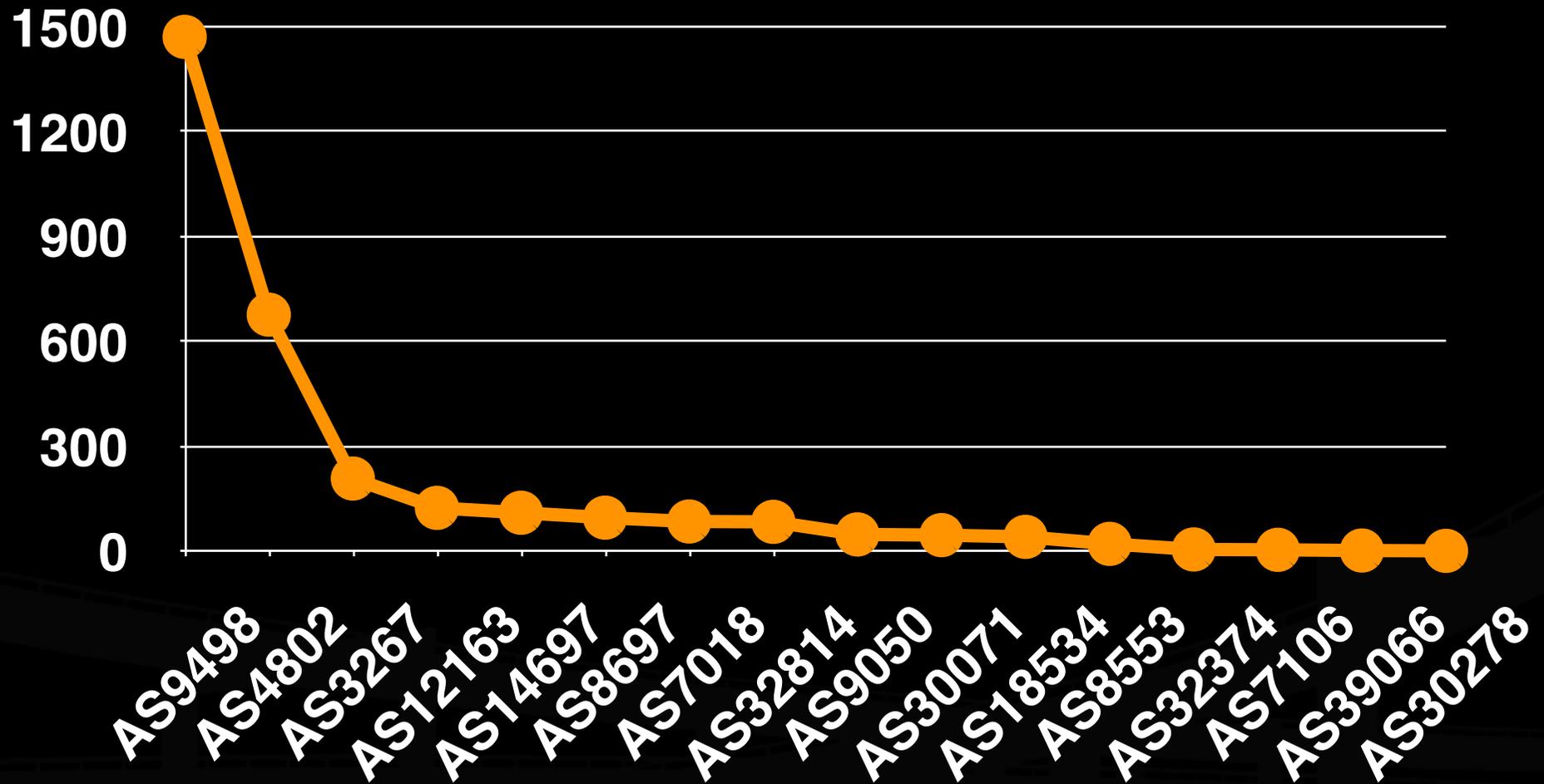
Examples:

1299 7018 12163 12163 12162 12163 12163 12163 12163
7018 65000 65001 7018 1239 4648 2764 9837 9476
11608 13768 21548 21548 21548 21548 7018 21548 36231

Non-contiguous Repeats



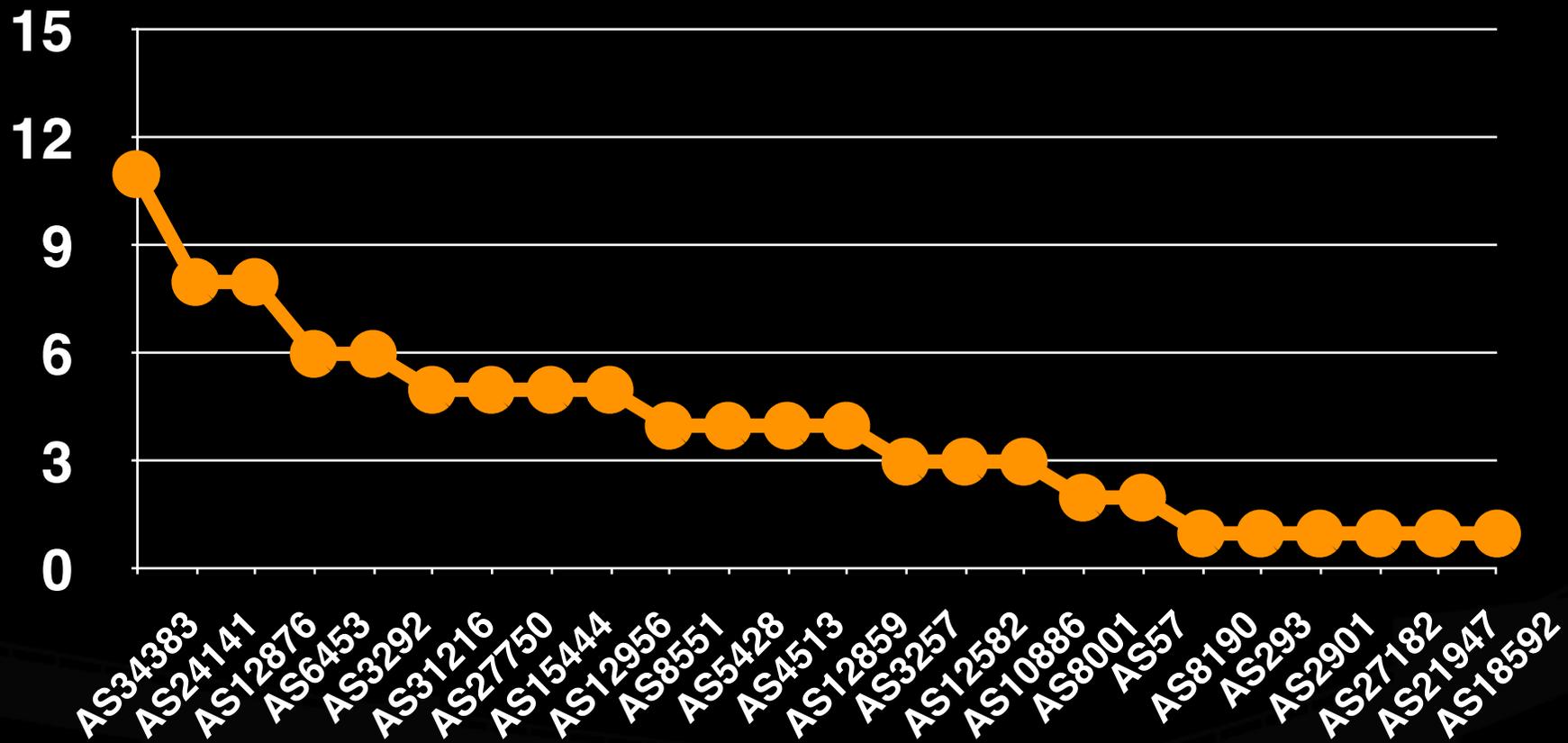
Non-contiguous Repeats



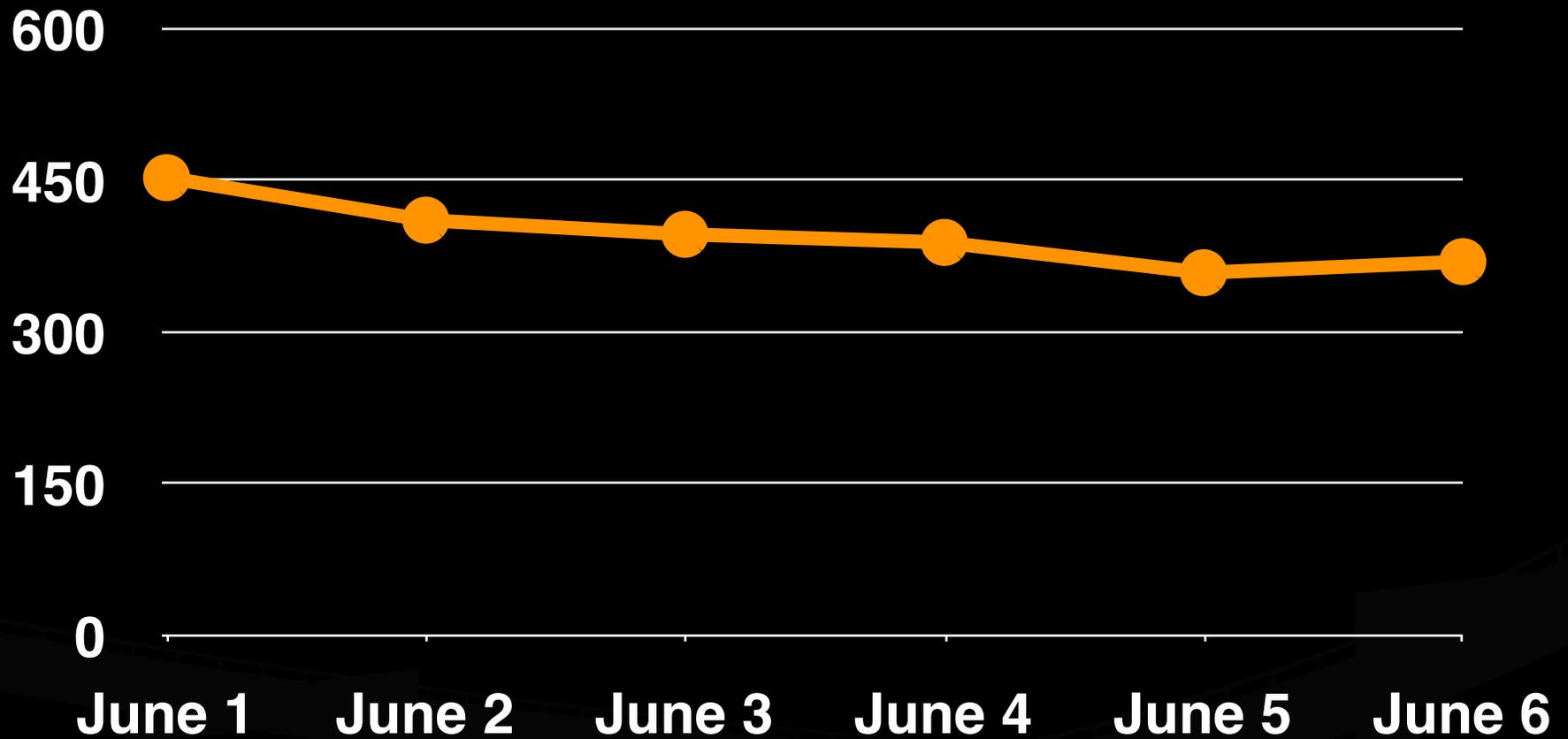
Private AS Number Leak

7018 65000 65001 7018 1239 4648 2764 9837 9476
14608 19029 2516 65000 4134

Private AS Number Leak



Private AS Number Leak

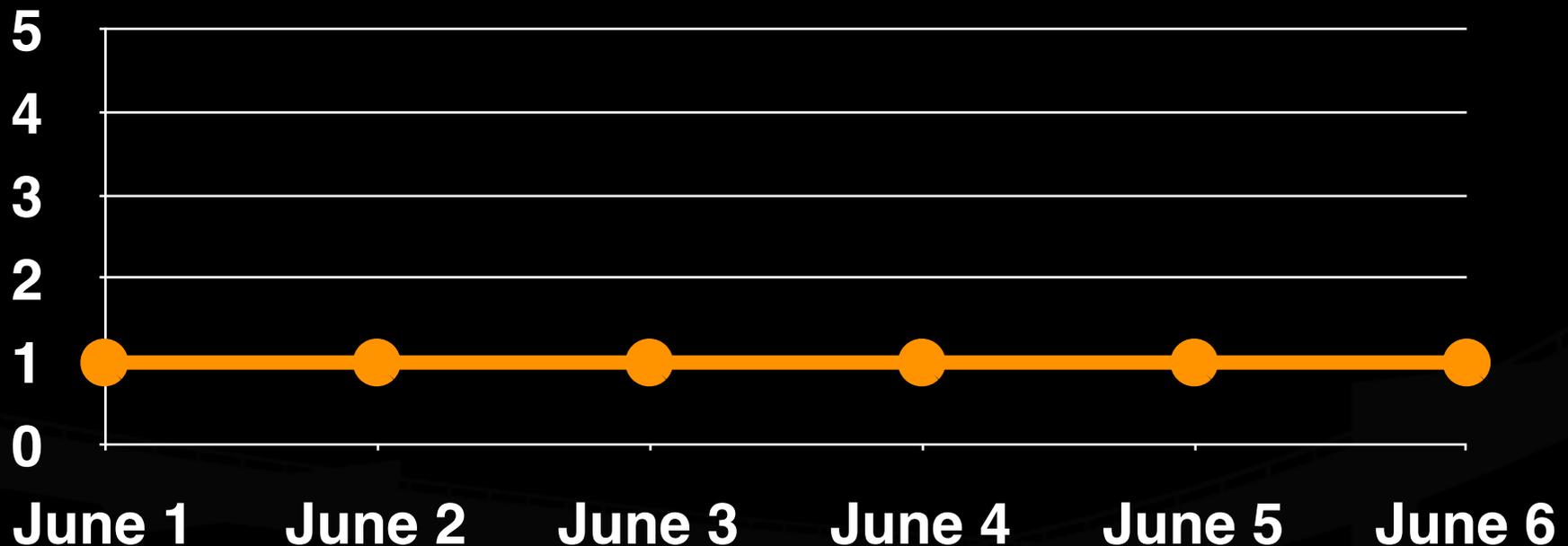


Using and Leaking Unallocated ASN

24587 is the only ASN leaking an unallocated ASN

81.17.39.128/27

3333 24587 **64500**



Adding a Candidate

The arbitrary method by which we seeded our list does not find content providers, only transit providers.

ATDN is reputed to be “tier-1” so we can test our proposition by adding them, and checking to see whether this yields additional anomalies...

Adding a Candidate

Adding ATDN (AOL Transit Data Network) to our list yields no additional observed anomalies. Thus they're probably fairly "tier-1."

Regional Differences

Reach was included in our seed list because it appeared frequently in Asian routing tables.

Looking only at Asian routing tables, Reach does not generate a significant number of anomalies.

Therefore, Reach is “tier-1” within the Asian region, but not globally.

Thanks, and Questions?

Copies of this presentation can be found
in PDF format at:

[http:// www.pch.net / resources / papers / bgp-aspath-analysis /](http://www.pch.net/resources/papers/bgp-aspath-analysis/)

Vijay Kumar Adhikari
Gaurab Raj Upadhaya
Bill Woodcock

bgp-anomalies@pch.net