BGP Hijacking 事件探討

臺灣大學

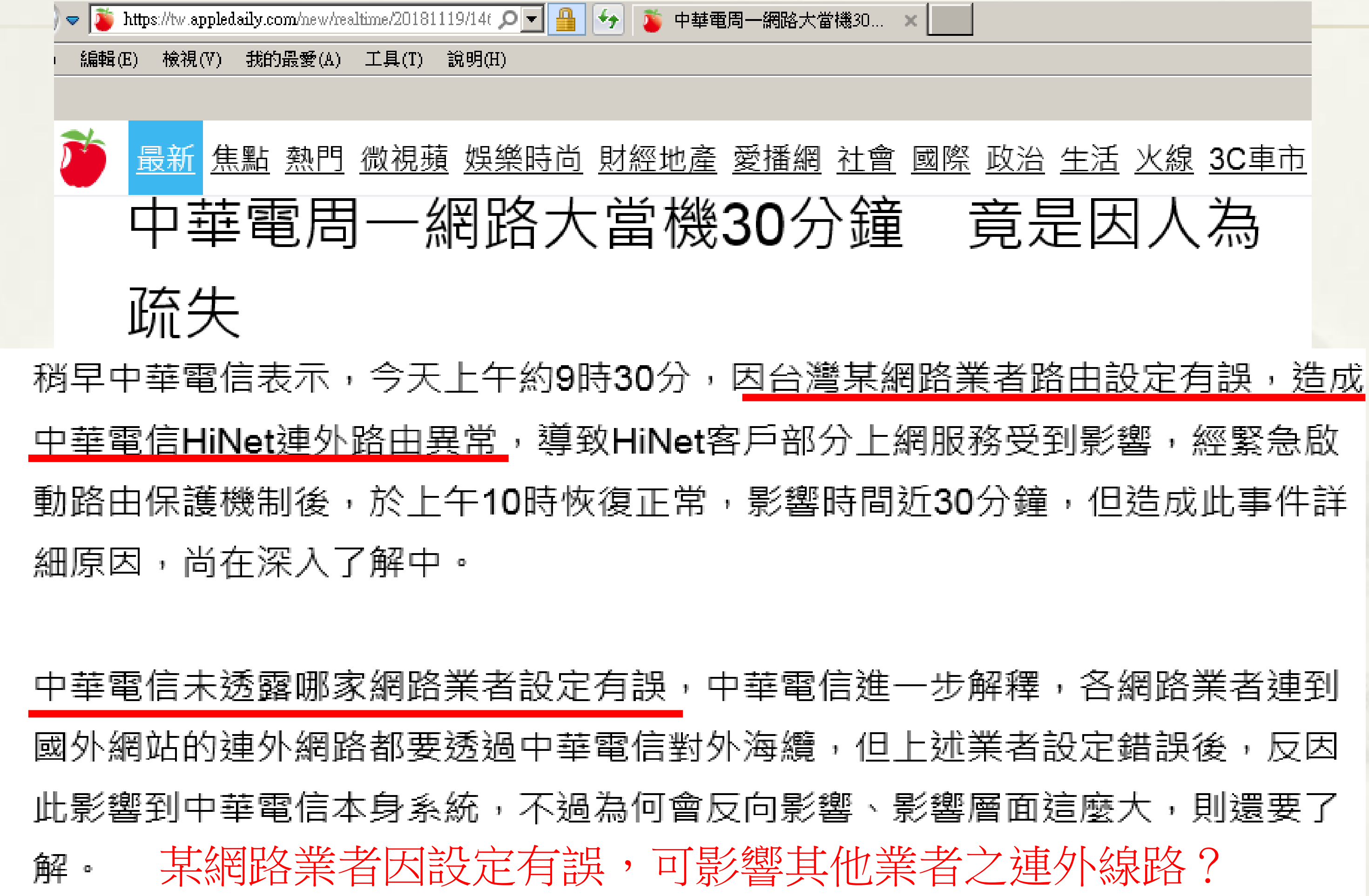
計資中心網路組

游子興

Agenda

- 從中華電信2018/11/19 網路大當機談起
- Six degrees of separation
  - Time To Live
  - AS-Path Length
- Threats of Border Gateway Protocol
  - BGP Outages
  - BGP Hijacking
  - BGP Leaks
- Prevention for BGP Hijacks & Leaks

2018/11/19 中華電信網路大當機



中華電周一網路大當機30分鐘　竟是因人為疏失

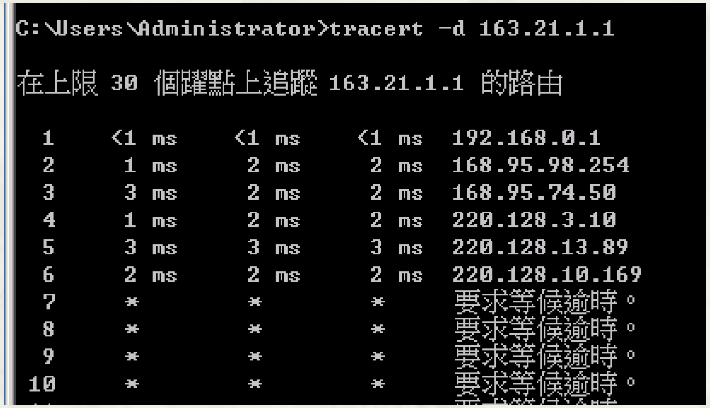
稍早中華電信表示，今天上午約9時30分，因台灣某網路業者路由設定有誤，造成中華電信HiNet連外路由異常，導致HiNet客戶部分上網服務受到影響，經緊急啟動路由保護機制後，於上午10時恢復正常，影響時間近30分鐘，但造成此事件詳細原因，尚在深入了解中。

中華電信未透露哪家網路業者設定有誤，中華電信進一步解釋，各網路業者連到國外網站的連外網路都要透過中華電信對外海纜，但上述業者設定錯誤後，反因此影響到中華電信本身系統，不過為何會反向影響、影響層面這麼大，則還要了解。　某網路業者因設定有誤，可影響其他業者之連外線路？

- https://tw.appledaily.com/new/realtime/20181119/1468986/

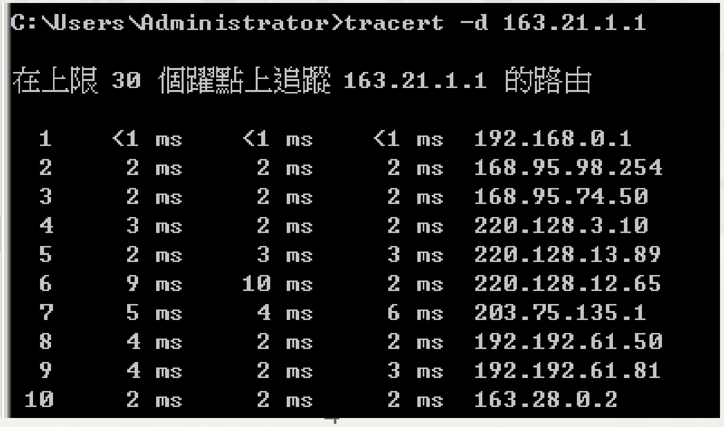
中華電信網路大當機
Trace Route

- From 中華電信光世代 To 臺北市網
- 發生異常時:



```
C:\Users\Administrator>tracert -d 163.21.1.1

在上限 30 個躍點上追蹤 163.21.1.1 的路由

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     1 ms     2 ms     2 ms  168.95.98.254
  3     3 ms     2 ms     2 ms  168.95.74.50
  4     1 ms     2 ms     2 ms  220.128.3.10
  5     3 ms     3 ms     3 ms  220.128.13.89
  6     2 ms     2 ms     2 ms  220.128.10.169
  7     *        *        *     要求等候逾時。
  8     *        *        *     要求等候逾時。
  9     *        *        *     要求等候逾時。
 10     *        *        *     要求等候逾時。
```

- 恢復正常後:



```
C:\Users\Administrator>tracert -d 163.21.1.1

在上限 30 個躍點上追蹤 163.21.1.1 的路由

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2     2 ms     2 ms     2 ms  168.95.98.254
  3     2 ms     2 ms     2 ms  168.95.74.50
  4     3 ms     2 ms     2 ms  220.128.3.10
  5     2 ms     3 ms     3 ms  220.128.13.89
  6     9 ms    10 ms     2 ms  220.128.12.65
  7     5 ms     4 ms     6 ms  203.75.135.1
  8     4 ms     2 ms     2 ms  192.192.61.50
  9     4 ms     2 ms     3 ms  192.192.61.81
 10     2 ms     2 ms     2 ms  163.28.0.2
```

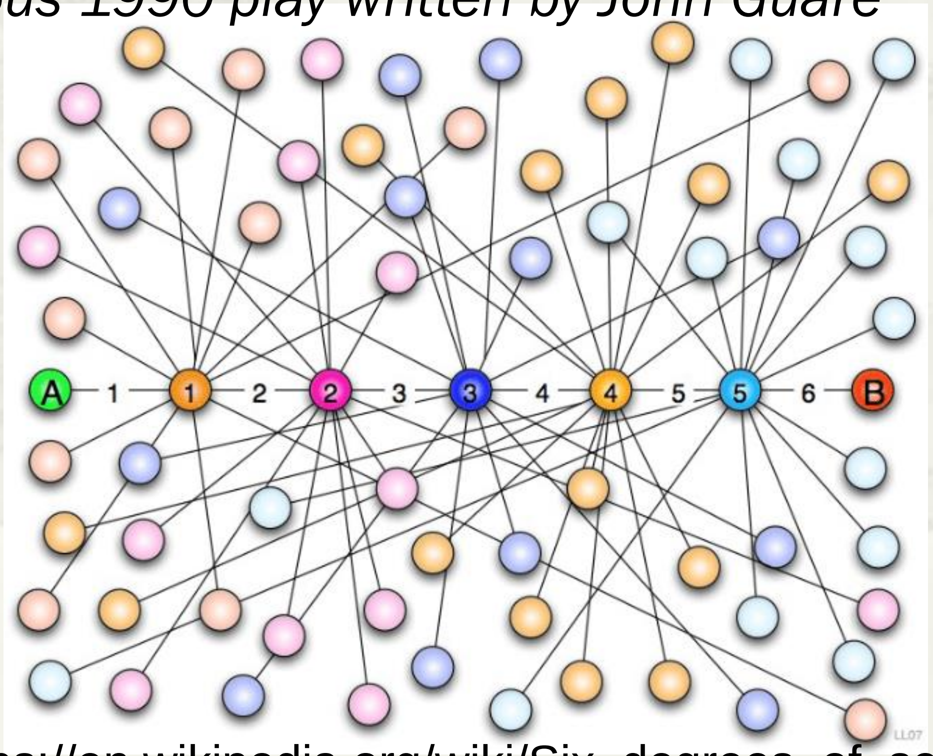
AS-Path Length

資工系老師
詢問 BGP AS-Path 長度限制

- ISP會丟掉AS路徑長度超過某個門檻值(比如255)的BGP更新訊息嗎?
- 如果會的話：
  - 為什麼您決定要丟掉這些AS路徑過長的訊息呢？有什麼特定的原因嗎？像是硬體的限制、資源運用的考量、或是避免潛在的相關攻擊等等
  - 目前AS路徑長度的上限門檻是多少呢？有哪些理由驅使您選擇這個門檻值呢？
  - 調高路徑長度門檻是可行的嗎？為什麼？那如果調高門檻可以增進整體BGP Protocol的安全性，您會考慮做出這個調整嗎？
- 如果不會的話：
  - 目前有任何遭遇到的攻擊或遇到的問題與BGP更新訊息內的異常路徑長度有關嗎？如果有的話，那是如何因應的呢？
  - 關於上面的問題或攻擊，忽略/丟棄那些異常路徑長度的BGP封包會是好的解法嗎？那您會考慮採用這種解法嗎？

Six degrees of separation

- all living things and everything else in the world are **six or fewer steps away from each other.**
- **a chain of "a friend of a friend**" statements can be made to **connect any two people in a maximum of six steps**.
- *Originally set out by Frigyes Karinthy in 1929 and popularized in an eponymous 1990 play written by John Guare*



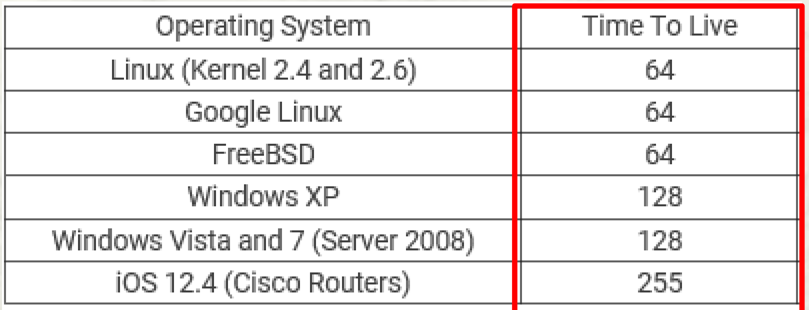
https://en.wikipedia.org/wiki/Six_degrees_of_separation

all living things and everything in 2018/12

- 地球人口
  - 7,662,668,199 (76億)
  - https://countrymeters.info/ct/World
- Facebook monthly active users
  - 2,320,000,000 (23億)
- IPv4 總數(2^32)
  - 4,294,967,296 (42億)
- BGP Prefixes 路由筆數
  - 784,801 (78萬)
- Autonomous System(AS) 總數
  - 63,400 (6萬3千)

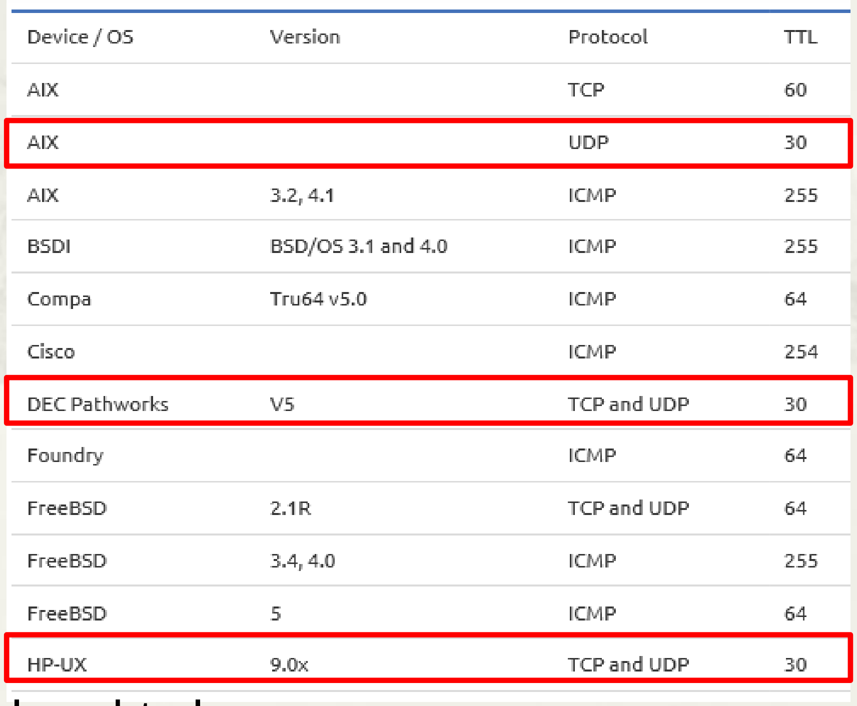
How to Verify?
Six degrees of separation

- Facebook
  - 至多僅需五個朋友即可關連所有 FB 帳戶?
- Trace Route Max Hops
  - IP Header: TTL max: 256(8-bit)



Operating System	Time To Live
Linux (Kernel 2.4 and 2.6)	64
Google Linux	64
FreeBSD	64
Windows XP	128
Windows Vista and 7 (Server 2008)	128
iOS 12.4 (Cisco Routers)	255

Android/Apple 64
Juniper/F5 254

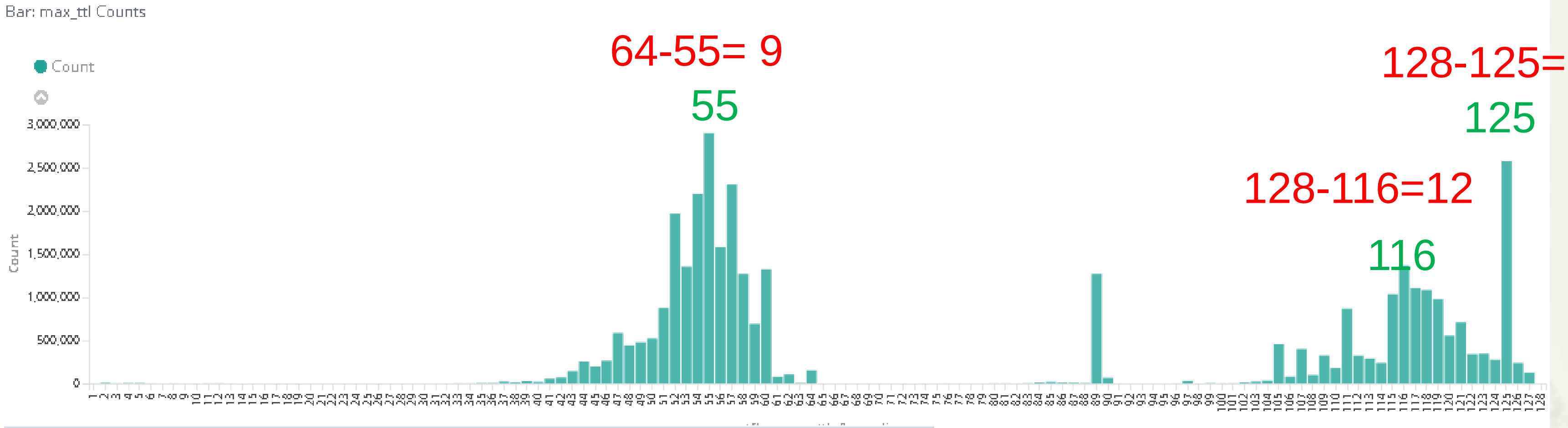


Device / OS	Version	Protocol	TTL
AIX		TCP	60
AIX		UDP	30
AIX	3.2, 4.1	ICMP	255
BSDI	BSD/OS 3.1 and 4.0	ICMP	255
Compa	Tru64 v5.0	ICMP	64
Cisco		ICMP	254
DEC Pathworks	V5	TCP and UDP	30
Foundry		ICMP	64
FreeBSD	2.1R	TCP and UDP	64
FreeBSD	3.4, 4.0	ICMP	255
FreeBSD	5	ICMP	64
HP-UX	9.0x	TCP and UDP	30

https://subinsb.com/default-device-ttl-values
http://noahdavids.org/self_published/TTL_values.html

How to Verify 6 degrees of separation? Time to Live (TTL)

- TTL: Internet to WAN (臺大 24 Hours)



64-55= 9

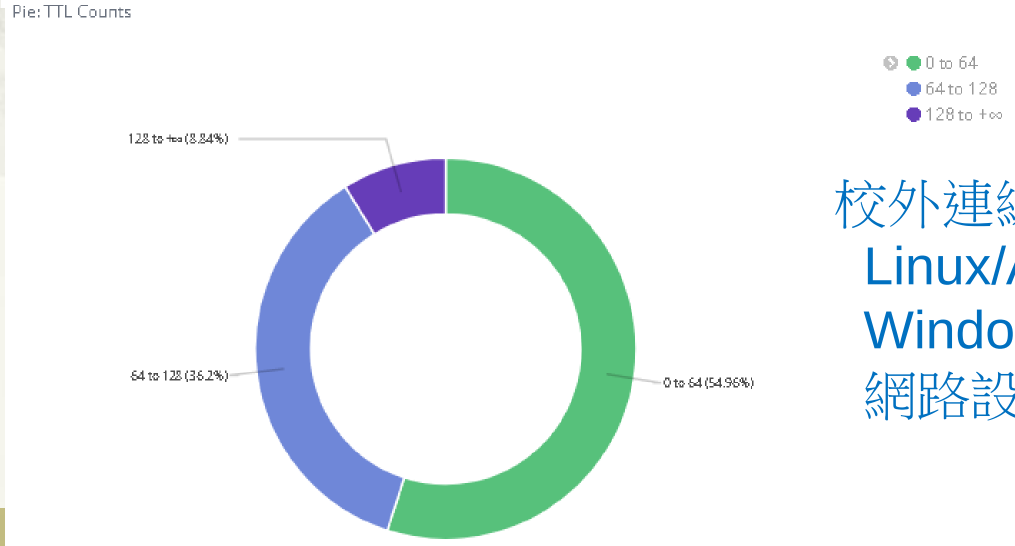
55

128-125= 3

125

128-116=12

116



校外連線裝置:

Linux/Android/Apple: 55%

Windows: 36%

網路設備: 9%

How to Verify 6 degrees of separation? Time to Live (TTL)

- TTL Counts: Internet to WAN (臺大 24 Hours)

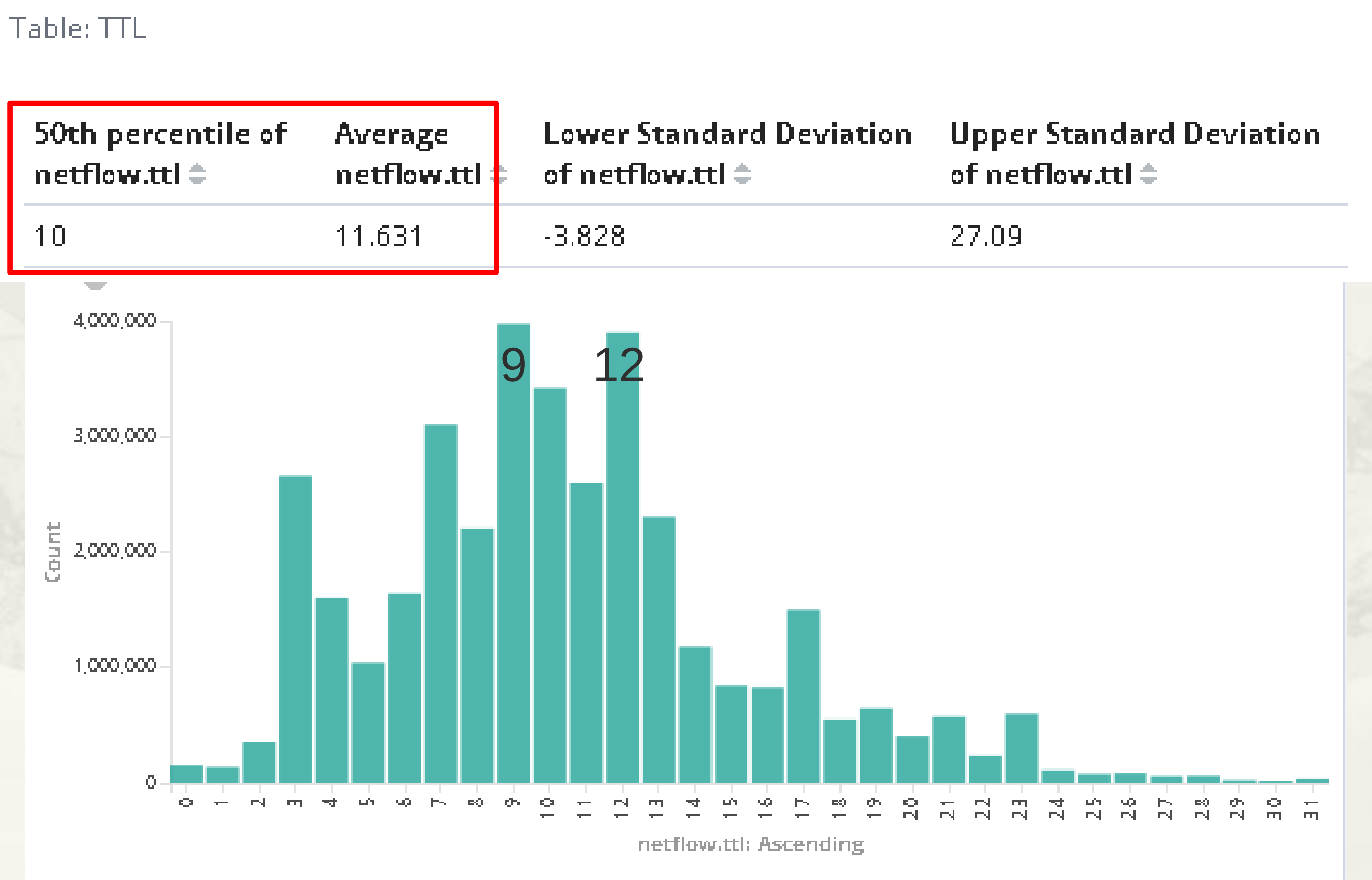
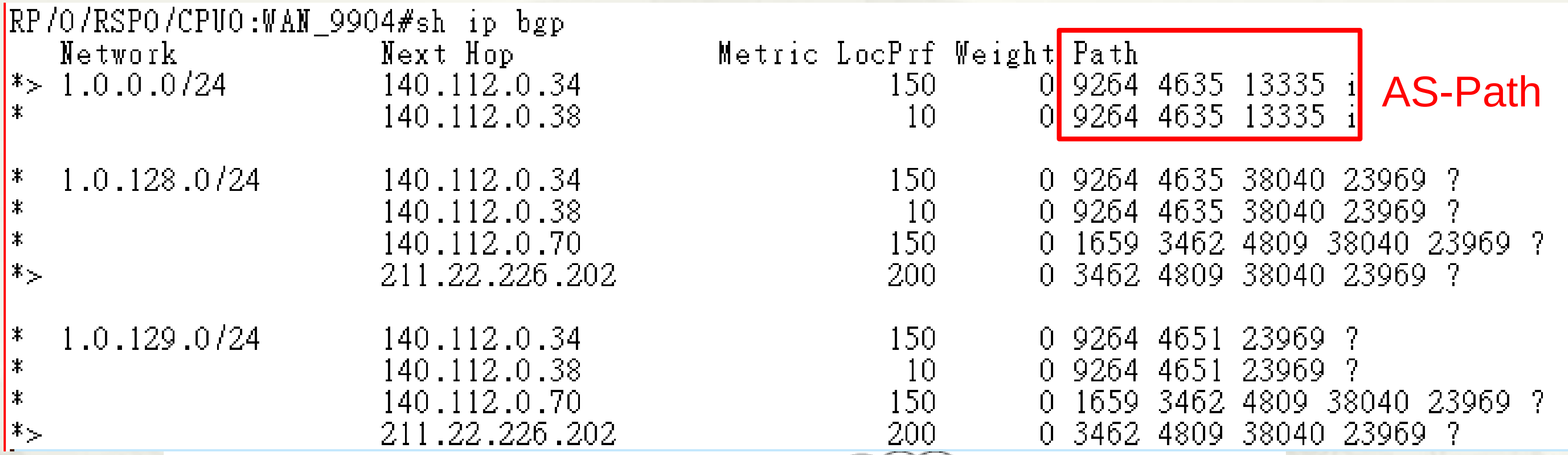


Table: TTL

50th percentile of netflow.ttl	Average netflow.ttl	Lower Standard Deviation of netflow.ttl	Upper Standard Deviation of netflow.ttl
10	11.631	-3.828	27.09

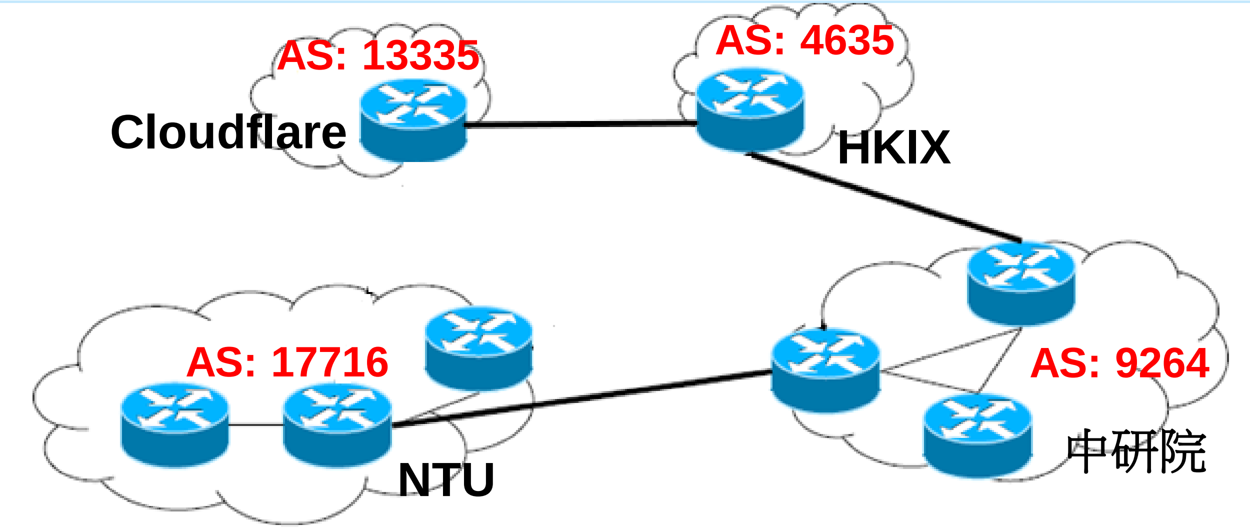
How to Verify 6 degrees of separation? BGP AS-Path

- BGP AS-Path

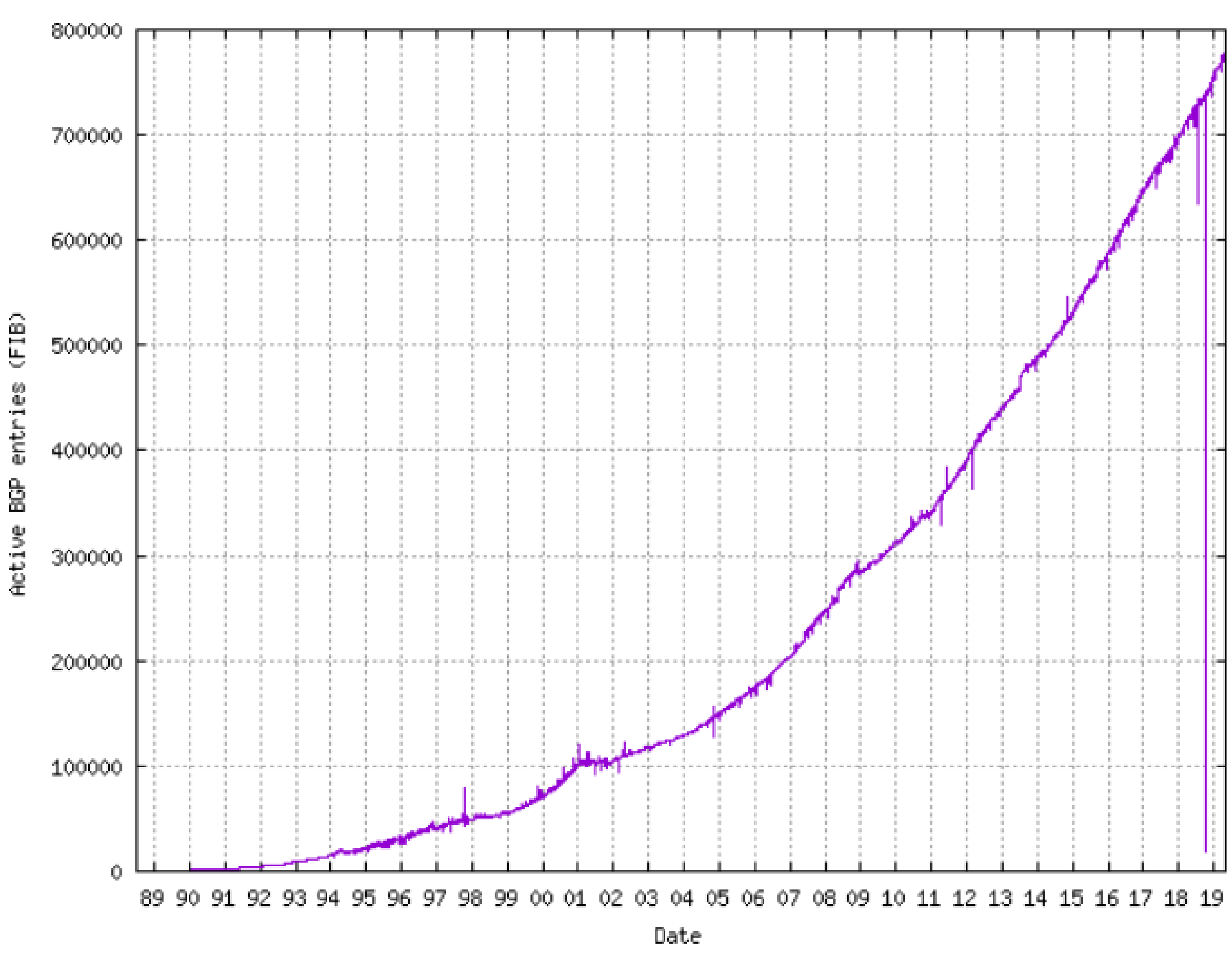


```
RP/0/RSP0/CPU0:WAN_9904#sh ip bgp
   Network            Next Hop            Metric LocPrf Weight Path
*> 1.0.0.0/24         140.112.0.34                   150      0 9264 4635 13335 i
*                     140.112.0.38                    10      0 9264 4635 13335 i

*  1.0.128.0/24       140.112.0.34                   150      0 9264 4635 38040 23969 ?
*                     140.112.0.38                    10      0 9264 4635 38040 23969 ?
*                     140.112.0.70                   150      0 1659 3462 4809 38040 23969 ?
*>                    211.22.226.202                 200      0 3462 4809 38040 23969 ?

*  1.0.129.0/24       140.112.0.34                   150      0 9264 4651 23969 ?
*                     140.112.0.38                    10      0 9264 4651 23969 ?
*                     140.112.0.70                   150      0 1659 3462 4809 38040 23969 ?
*>                    211.22.226.202                 200      0 3462 4809 38040 23969 ?
```

AS-Path



Total BGP Routing Table(Prefixes)



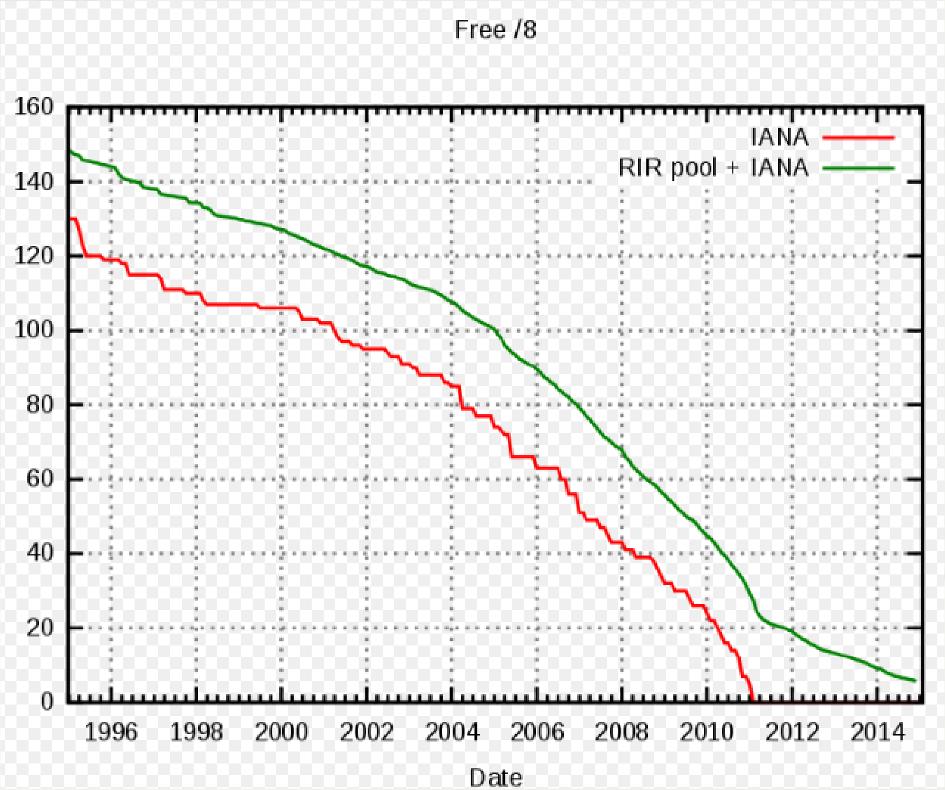
80萬

Plot Range: 30-Jun-1988 1430 to 30-Apr-2019 0730

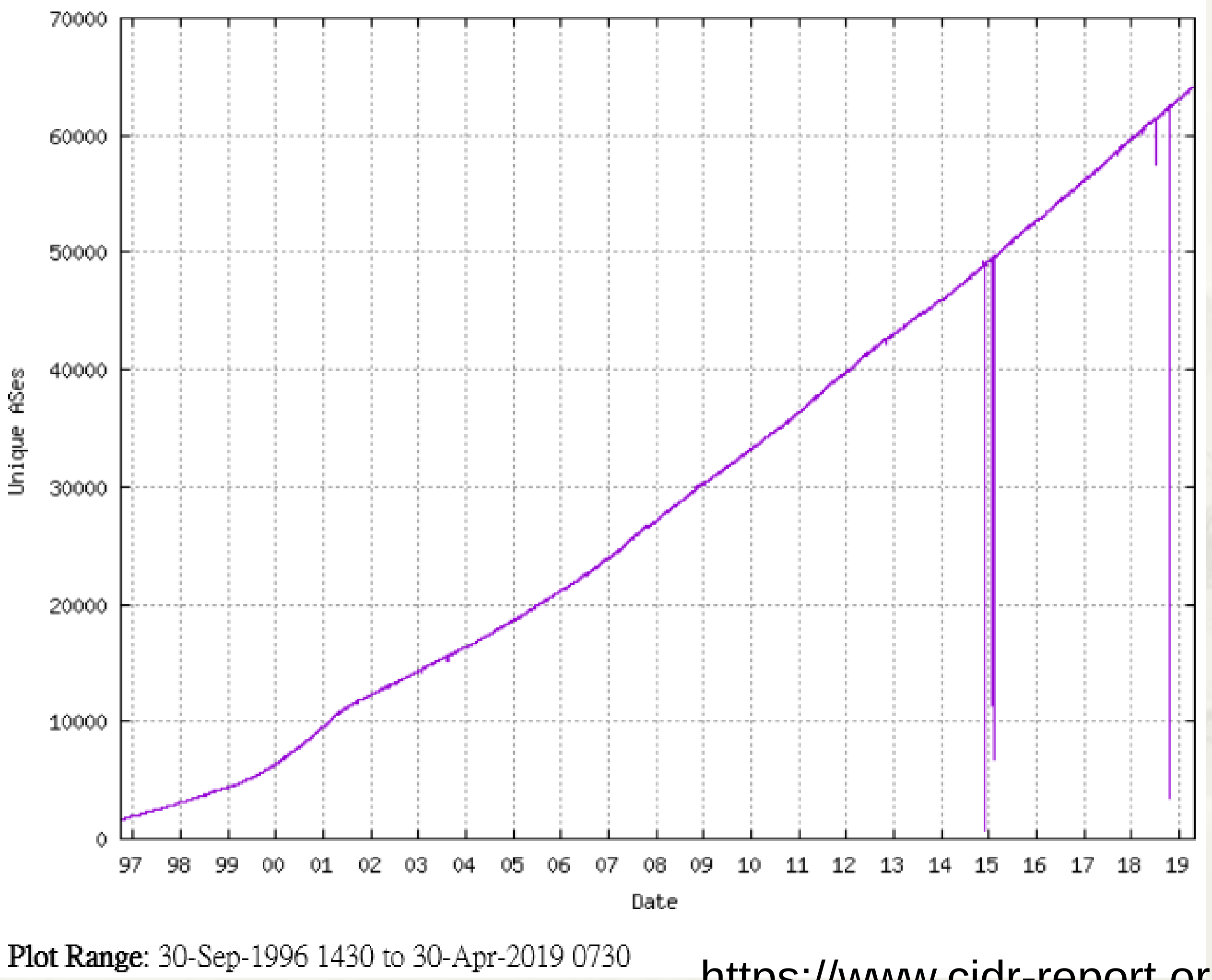
https://www.cidr-report.org/as2.0/
BGP Table Size

IPv4 address exhaustion

- IPv4 address exhaustion that occurred **before 2011 and 2015** did not slow down the speed of IPv4 table growth, instead it **accelerated the fragmentation of IPv4 space.**
- https://en.wikipedia.org/wiki/IPv4_address_exhaustion



Total BGP AS counts

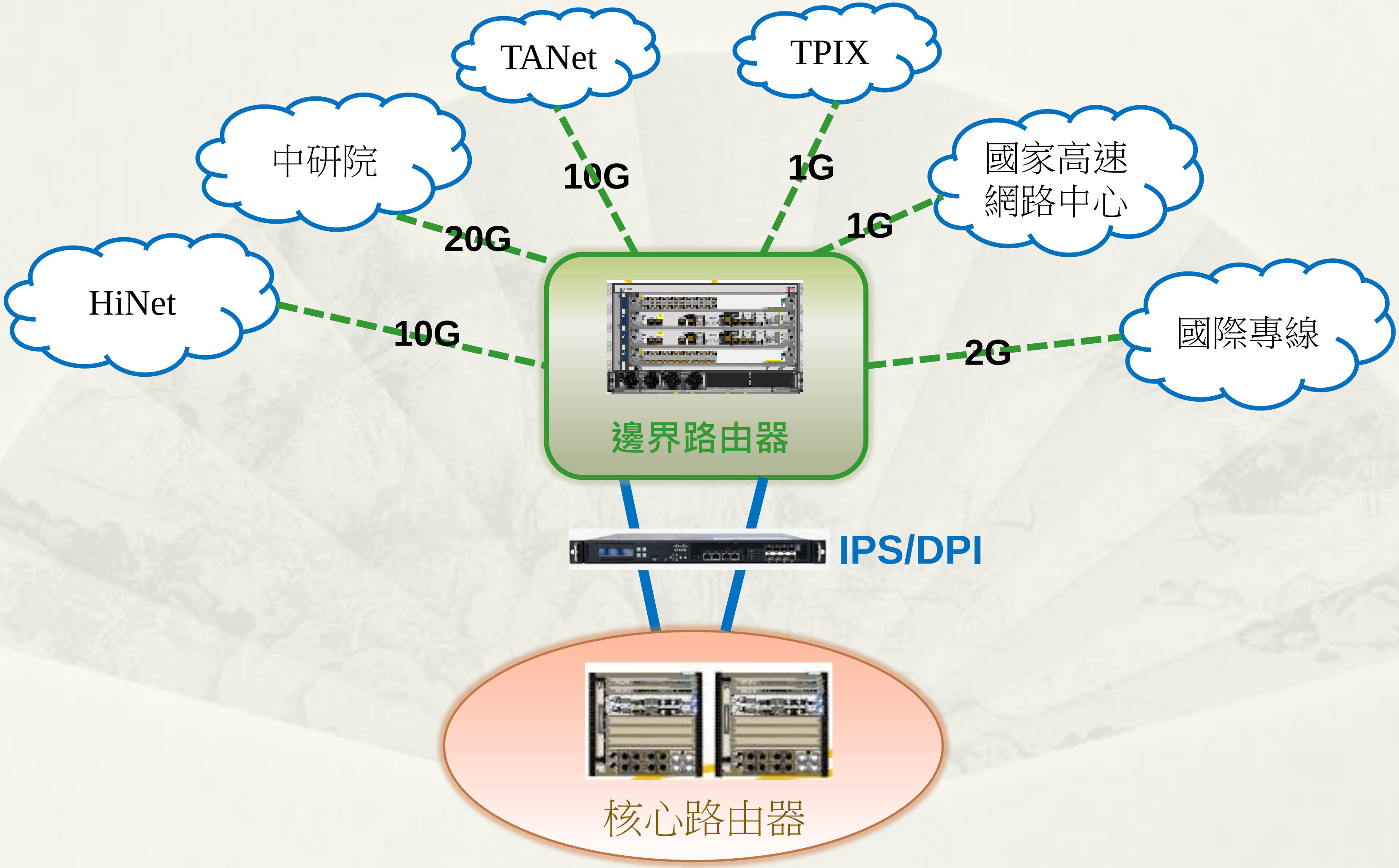


Plot Range: 30-Sep-1996 1430 to 30-Apr-2019 0730

7萬

https://www.cidr-report.org/as2.0/
AS count

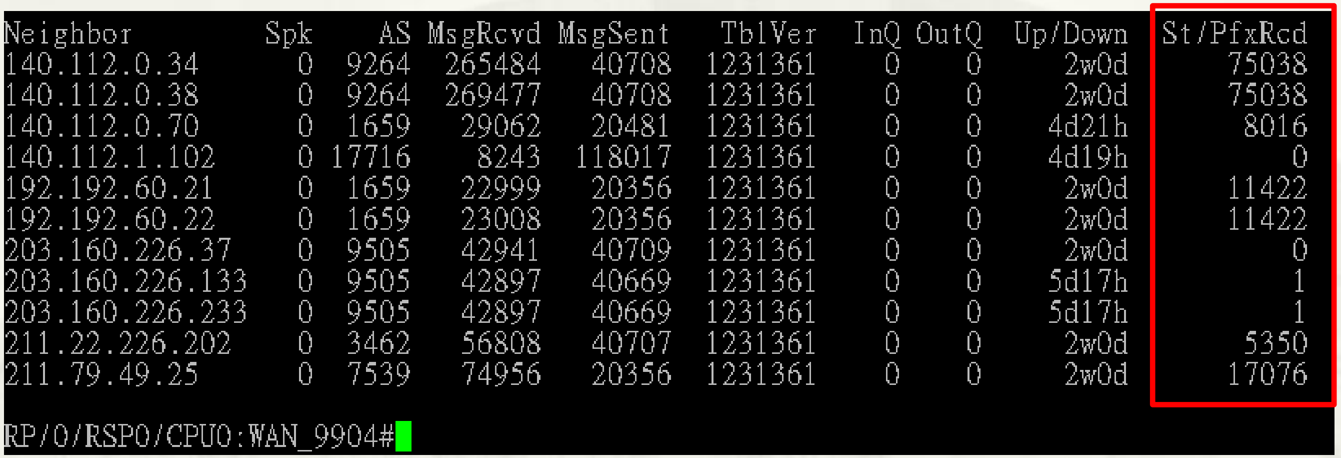
臺大對外網路架構圖


TANet
TPIX
中研院
國家高速網路中心
HiNet
國際專線
10G
1G
20G
1G
10G
2G
邊界路由器
IPS/DPI
核心路由器

NTU WAN Router

- Total Received BGP Prefixes: 116,902

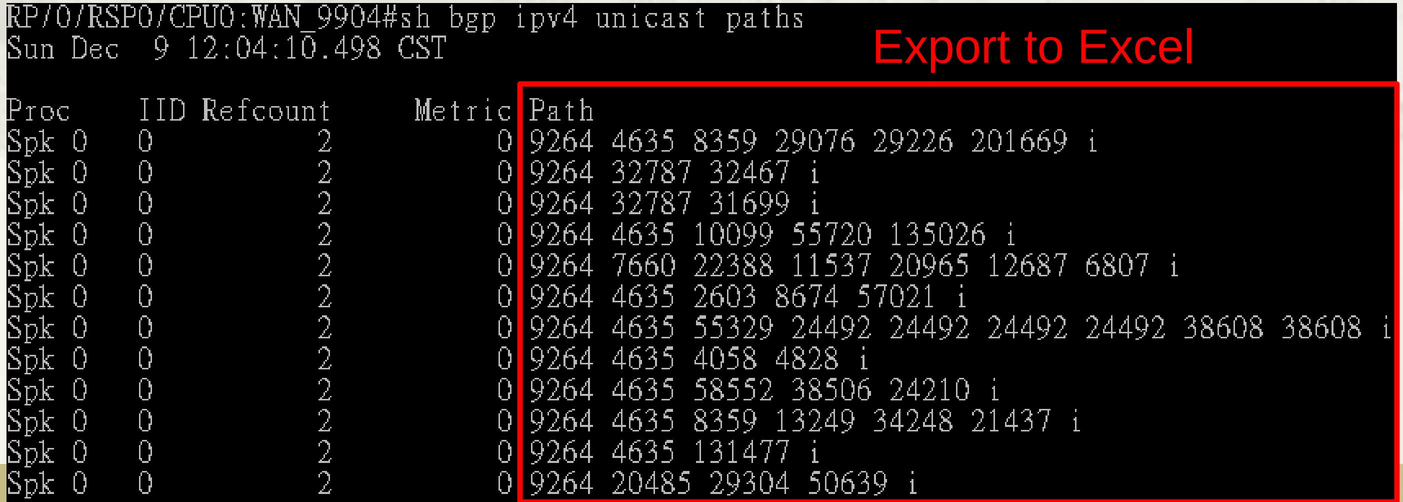
Total Prefix: 15%



```
Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
140.112.0.34      0  9264  265484   40708  1231361    0    0     2w0d      75038
140.112.0.38      0  9264  269477   40708  1231361    0    0     2w0d      75038
140.112.0.70      0  1659   29062   20481  1231361    0    0    4d21h       8016
140.112.1.102     0 17716    8243  118017  1231361    0    0    4d19h          0
192.192.60.21     0  1659   22999   20356  1231361    0    0     2w0d      11422
192.192.60.22     0  1659   23008   20356  1231361    0    0     2w0d      11422
203.160.226.37    0  9505   42941   40709  1231361    0    0     2w0d          0
203.160.226.133   0  9505   42897   40669  1231361    0    0    5d17h          1
203.160.226.233   0  9505   42897   40669  1231361    0    0    5d17h          1
211.22.226.202    0  3462   56808   40707  1231361    0    0     2w0d       5350
211.79.49.25      0  7539   74956   20356  1231361    0    0     2w0d      17076

RP/0/RSP0/CPU0:WAN_9904#
```

- Total different AS-Paths: 35,157

Total AS: 50%



Export to Excel

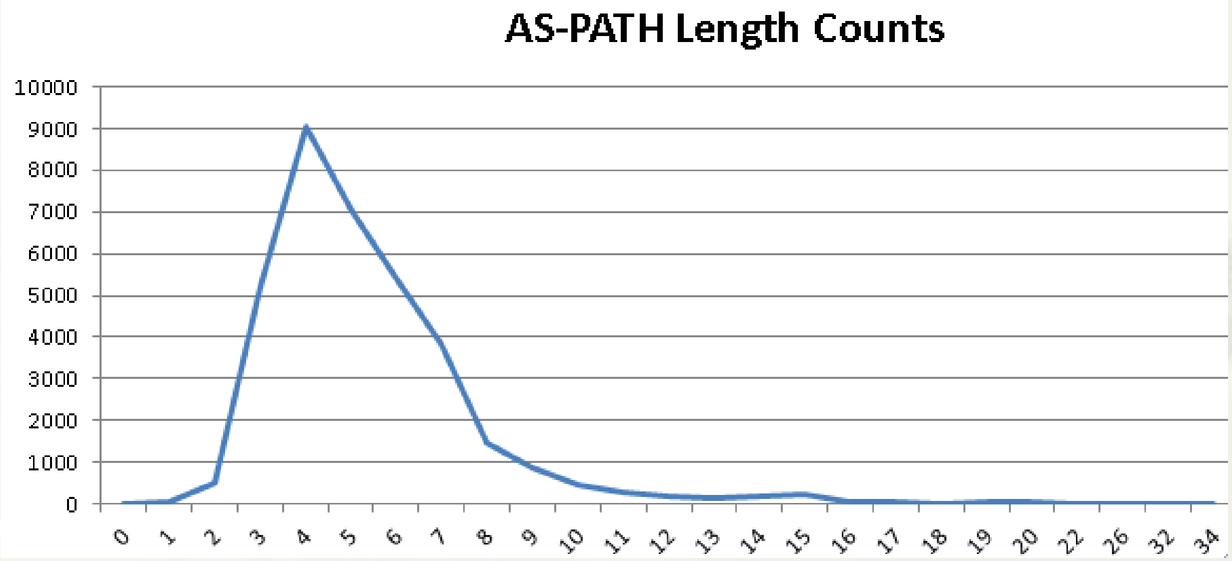
```
RP/0/RSP0/CPU0:WAN_9904#sh bgp ipv4 unicast paths
Sun Dec  9 12:04:10.498 CST

Proc    IID Refcount     Metric Path
Spk 0   0          2          0 9264 4635 8359 29076 29226 201669 i
Spk 0   0          2          0 9264 32787 32467 i
Spk 0   0          2          0 9264 32787 31699 i
Spk 0   0          2          0 9264 4635 10099 55720 135026 i
Spk 0   0          2          0 9264 7660 22388 11537 20965 12687 6807 i
Spk 0   0          2          0 9264 4635 2603 8674 57021 i
Spk 0   0          2          0 9264 4635 55329 24492 24492 24492 24492 38608 38608 i
Spk 0   0          2          0 9264 4635 4058 4828 i
Spk 0   0          2          0 9264 4635 58552 38506 24210 i
Spk 0   0          2          0 9264 4635 8359 13249 34248 21437 i
Spk 0   0          2          0 9264 4635 131477 i
Spk 0   0          2          0 9264 20485 29304 50639 i
```

NTU WAN Router AS-Path Length 統計

AS-Path Length	Counts
1	45
2	523
3	5214
4	9045
5	7050
6	5417
7	3838
8	1477
9	877
10	471
11	283
12	185
13	135
14	181
15	225
16	53
17	36
18	18
19	37
20	33
22	3
26	3
32	3
34	3

Average	5.4
Median	5

恰好符合: 6 degrees of separation

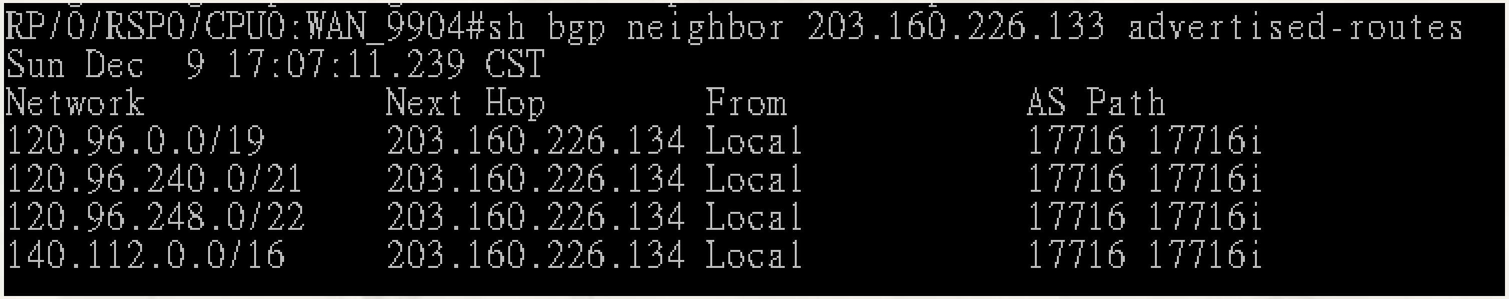


NTU WAN Router
Top 3 Max AS-Path Length

- AS-Path Length: 34
  - 9264 4635 8359 29076 196691 196691 196691
    196691 196691 196691 196691 196691 196691 196691
    196691 196691 196691 196691 196691 196691 196691
    196691 196691 196691 196691 196691 198130 198130
    198130 198130 198130 198130 198130 198130 i
- AS-Path Length: 32
  - 9264 15412 12880 12880 12880 12880 12880 12880
    12880 12880 12880 12880 12880 43754 202269
    202269 202269 202269 202269 202269 202269 202269
    202269 202269 202269 202269 202269 202269 202269
    202269 202269 202269 i
- AS-Path Length: 26
  - 9264 15412 45899 45557 45557 45557 45557 45557
    45557 45557 45557 45557 45557 45557 45557 45557
    45557 45557 45557 45557 45557 45557 45557 45557
    45557 45557 i

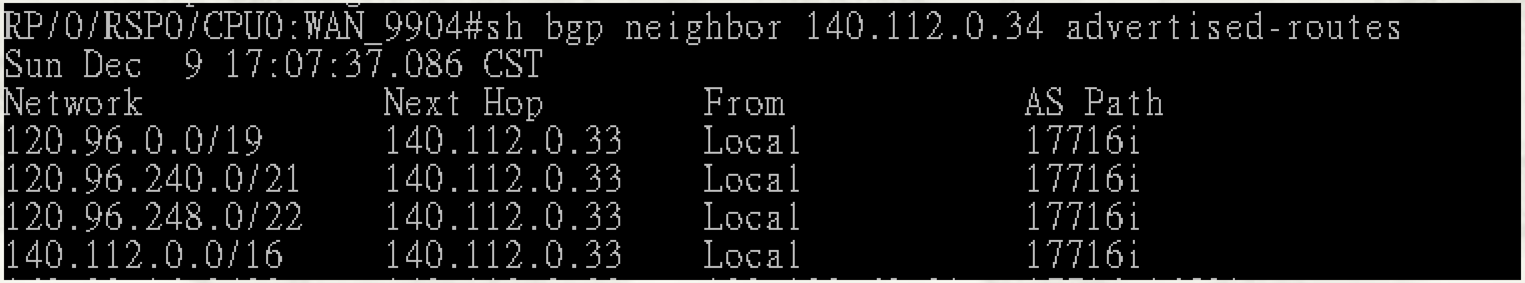
NTU WAN Router
BGP AS prepend

- Advertisement to TWGate



```
RP/0/RSP0/CPU0:WAN_9904#sh bgp neighbor 203.160.226.133 advertised-routes
Sun Dec  9 17:07:11.239 CST
Network            Next Hop        From            AS Path
120.96.0.0/19      203.160.226.134 Local           17716 17716i
120.96.240.0/21    203.160.226.134 Local           17716 17716i
120.96.248.0/22    203.160.226.134 Local           17716 17716i
140.112.0.0/16     203.160.226.134 Local           17716 17716i
```

- Advertisement to 中研院



```
RP/0/RSP0/CPU0:WAN_9904#sh bgp neighbor 140.112.0.34 advertised-routes
Sun Dec  9 17:07:37.086 CST
Network            Next Hop        From            AS Path
120.96.0.0/19      140.112.0.33    Local           17716i
120.96.240.0/21    140.112.0.33    Local           17716i
120.96.248.0/22    140.112.0.33    Local           17716i
140.112.0.0/16     140.112.0.33    Local           17716i
```

AS-Path too long Conclusion

- 現今 Internet 環境中, ISP 彼此互連的情況非常頻繁, 因此不大可能發生到達某 ASN 需超過 255 AS-Path 才能抵達的情況.
- 目前 TANet 所有骨幹路由器中並無限制 AS Path長度設定.
- Limit the number of AS path to prevent the router from expending too much memory when it stores a very long AS path
  - (config)# router bgp 1659
  - (config-router)# maxas-limit 50

Threats of Border Gateway Protocol

Threats of Border Gateway Protocol

- BGP: antiquated design protocol
  - Lack of adoption of encryption or automatic verification methods.
- Common Problems
  - BGP Overage
  - BGP Hijacking
  - BGP Leaks

BGP Outages

- 超過時間未收到 BGP 更新訊息
- The default advertisements
  - 30 seconds for eBGP
  - 5 seconds for iBGP.

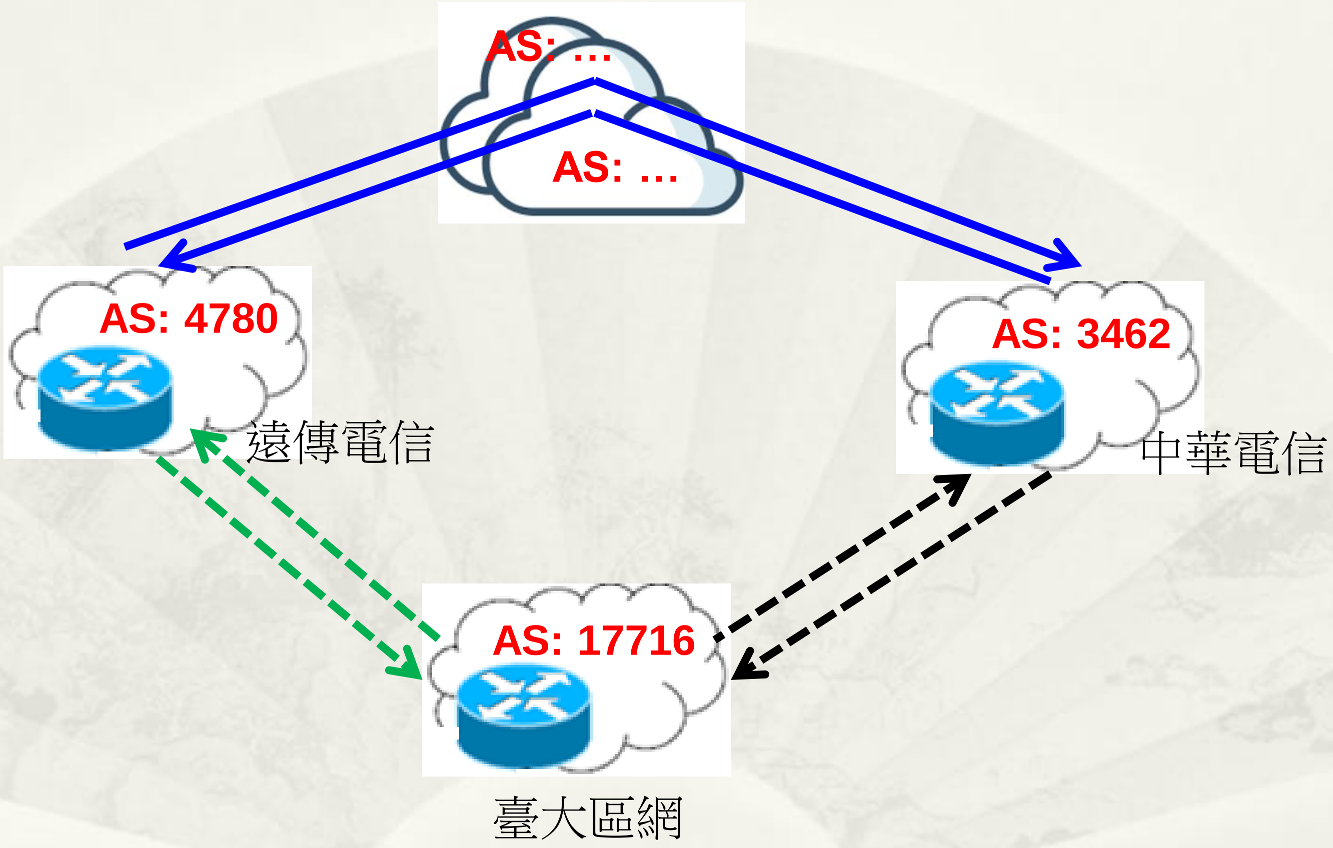
BGP Hijacking

- Partial BGP Hijacking
  - Two AS announce an identical IP prefix with the same prefix length.
- Complete BGP Hijacking
  - An AS announces a more specific IP prefix than the actual owner of the prefix.

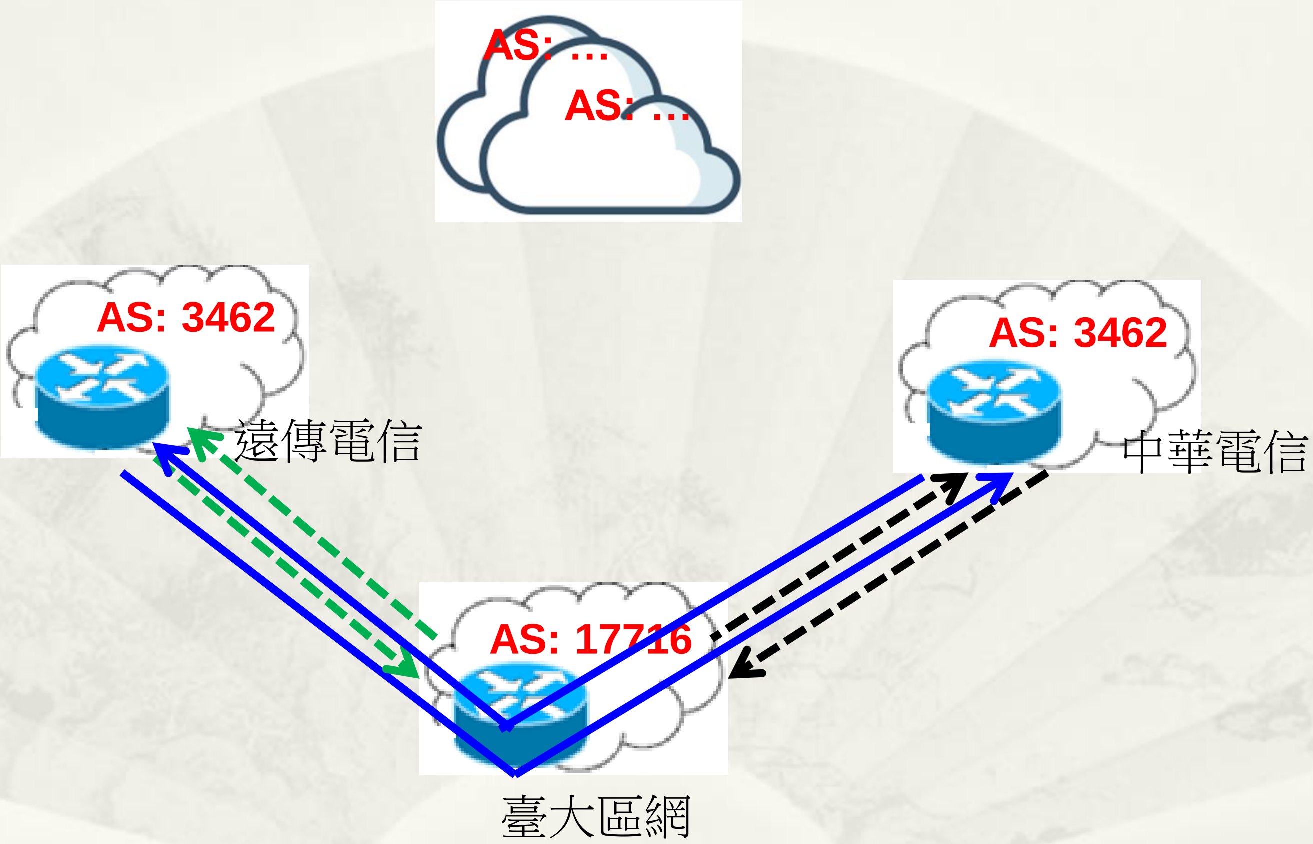
BGP Leaks

- an announcement from an AS of a learned BGP route to another AS.
- The propagation of routing announcements beyond their intended scope.
- Leaks can be accidental or malicious but most often arise from accidental misconfigurations.
- *Ref. RFC 7908 definition*

No BGP Leaks

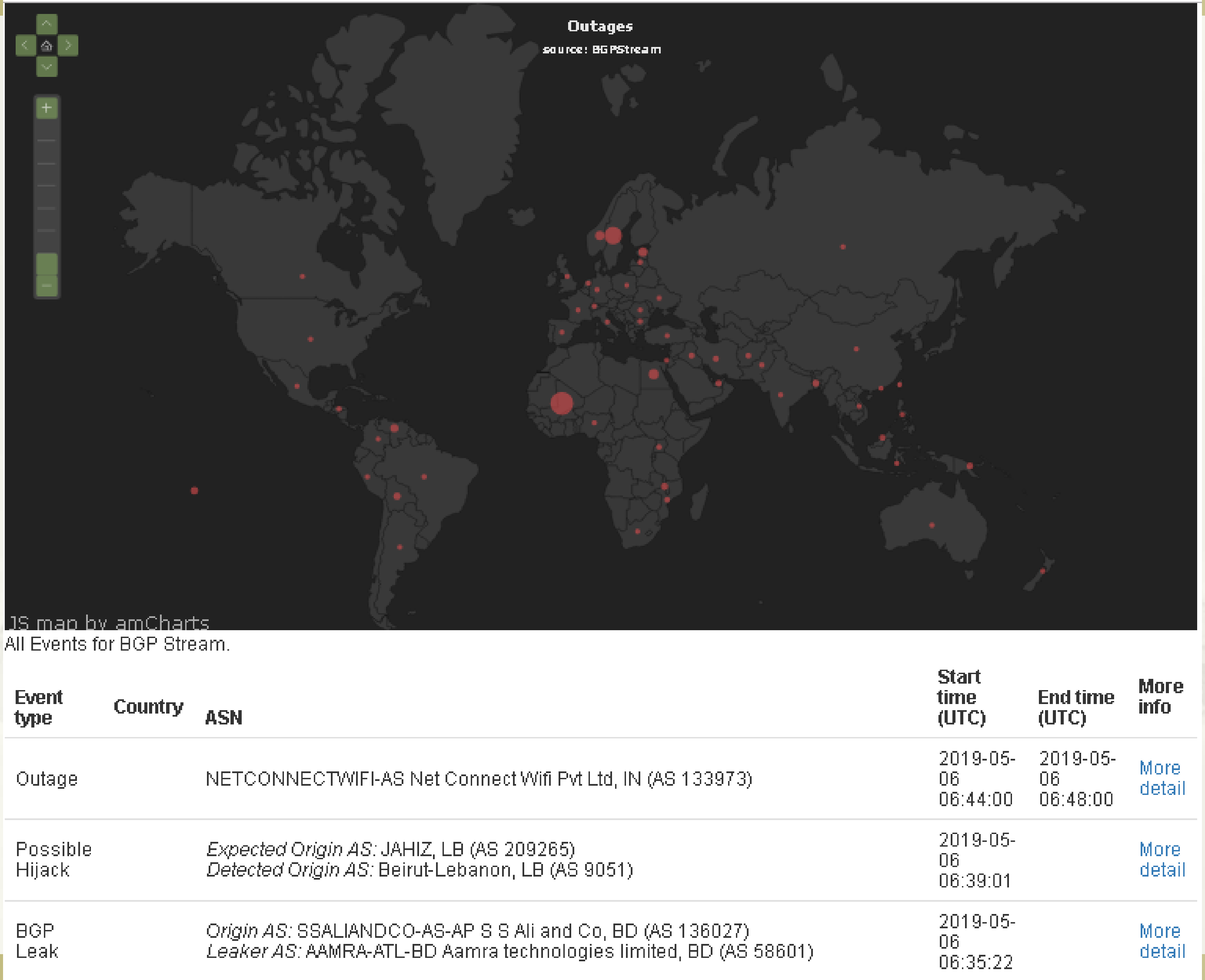


BGP Leaks



BGP Stream Web Site

- https://bgpstream.com/
- BGP Stream is a free resource for receiving alerts about hijacks, leaks, and outages in the Border Gateway Protocol.
- Monitor and compare the changes of AS-Path from it’s collector peers.
- It can not cover 100% changes of AS-Path in the world.

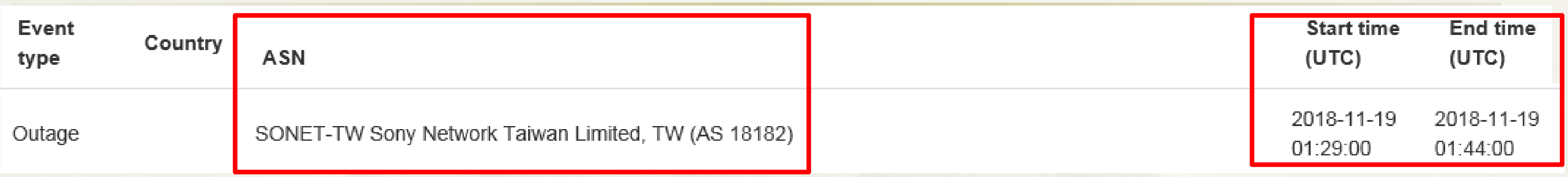


All Events for BGP Stream.

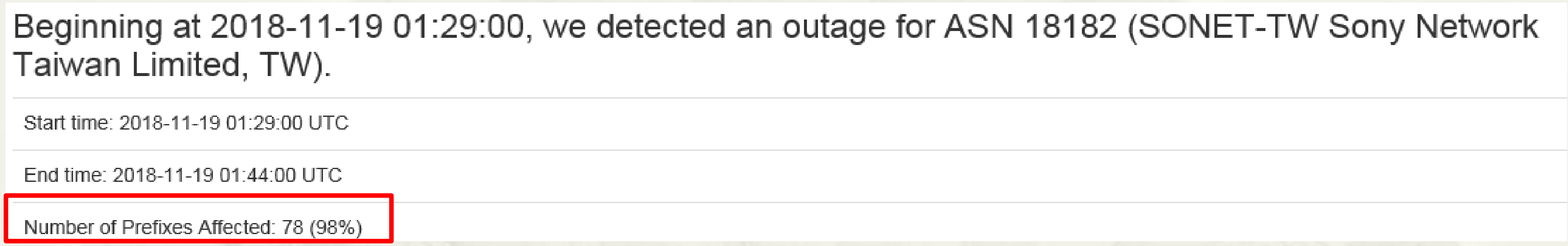
Event type	Country	ASN	Start time (UTC)	End time (UTC)	More info
Outage		NETCONNECTWIFI-AS Net Connect Wifi Pvt Ltd, IN (AS 133973)	2019-05-06 06:44:00	2019-05-06 06:48:00	More detail
Possible Hijack		*Expected Origin AS:* JAHIZ, LB (AS 209265) *Detected Origin AS:* Beirut-Lebanon, LB (AS 9051)	2019-05-06 06:39:01		More detail
BGP Leak		*Origin AS:* SSALIANDCO-AS-AP S S Ali and Co, BD (AS 136027) *Leaker AS:* AAMRA-ATL-BD Aamra technologies limited, BD (AS 58601)	2019-05-06 06:35:22		More detail

BGP Outage

BGP Outage
ASN 18182 (SONET)



Event type	Country	ASN	Start time (UTC)	End time (UTC)
Outage		SONET-TW Sony Network Taiwan Limited, TW (AS 18182)	2018-11-19 01:29:00	2018-11-19 01:44:00



Beginning at 2018-11-19 01:29:00, we detected an outage for ASN 18182 (SONET-TW Sony Network Taiwan Limited, TW).

Start time: 2018-11-19 01:29:00 UTC

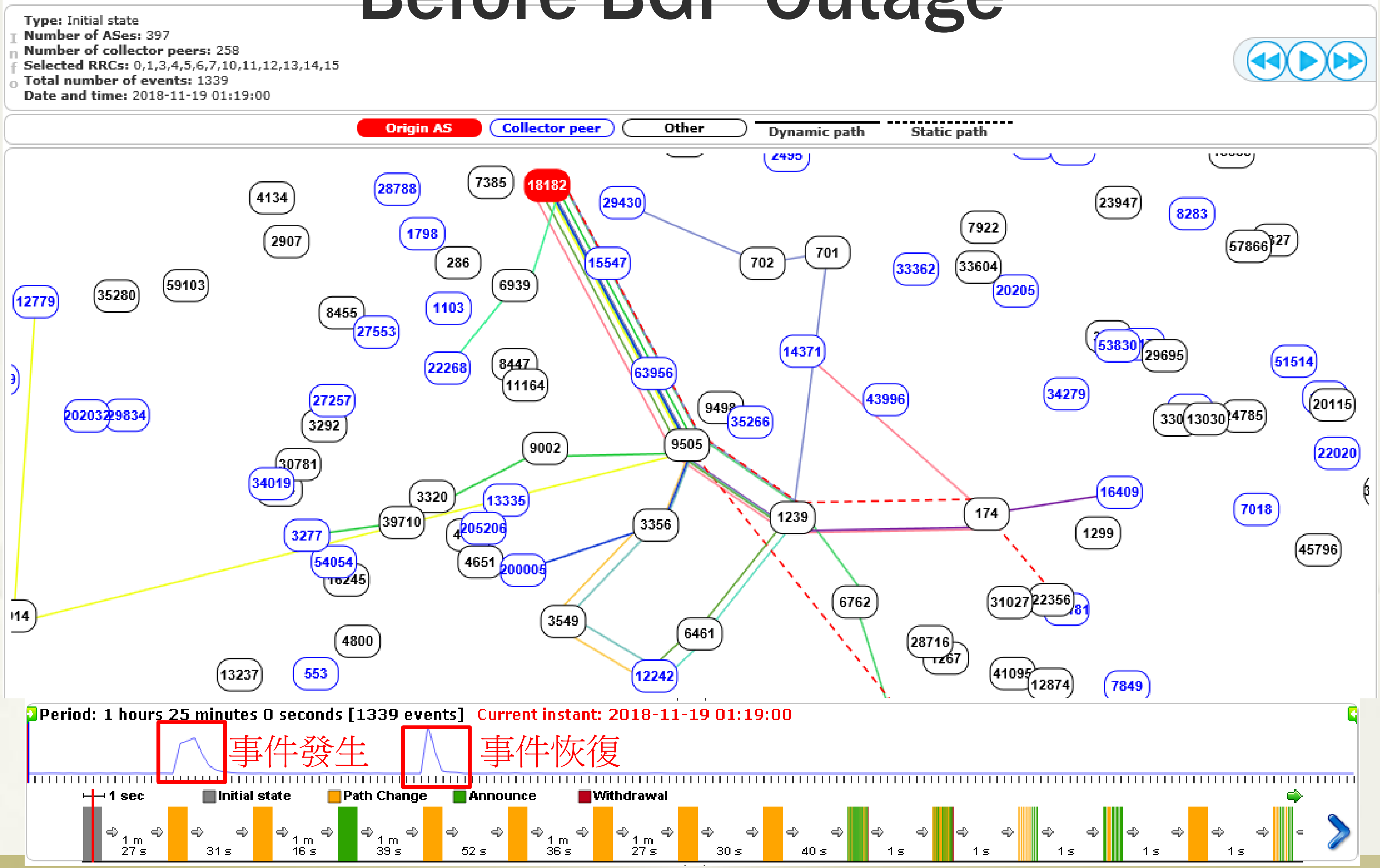
End time: 2018-11-19 01:44:00 UTC

Number of Prefixes Affected: 78 (98%)

https://bgpstream.com/event/160356

ASN 18182

Before BGP Outage



Type: Initial state
Number of ASes: 397
Number of collector peers: 258
Selected RRCs: 0,1,3,4,5,6,7,10,11,12,13,14,15
Total number of events: 1339
Date and time: 2018-11-19 01:19:00

Origin AS | Collector peer | Other | Dynamic path | Static path

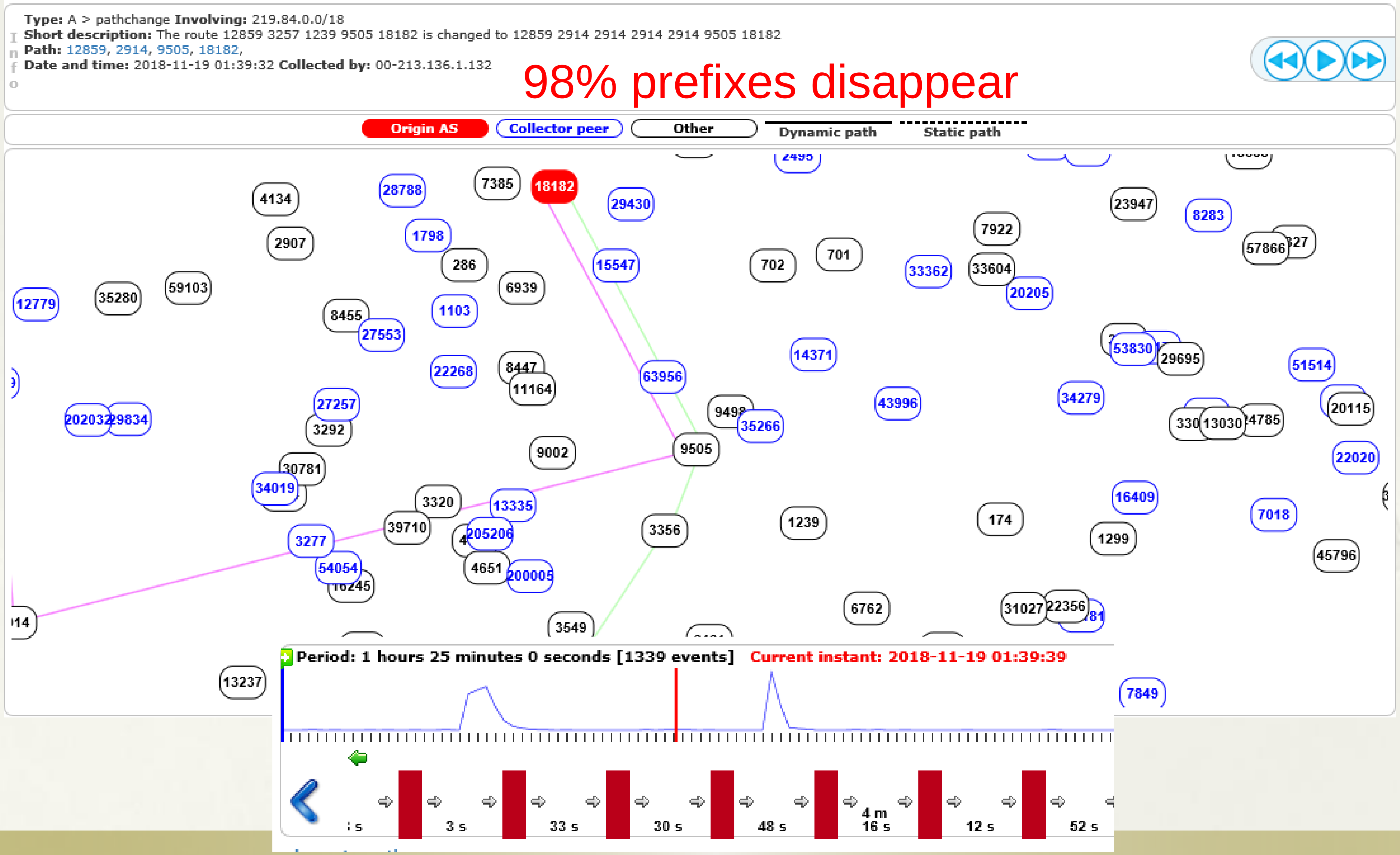
Period: 1 hours 25 minutes 0 seconds [1339 events] Current instant: 2018-11-19 01:19:00

事件發生

事件恢復

1 sec | ▨ Initial state | 🟧 Path Change | 🟩 Announce | 🟥 Withdrawal

ASN 18182
BGP Outage

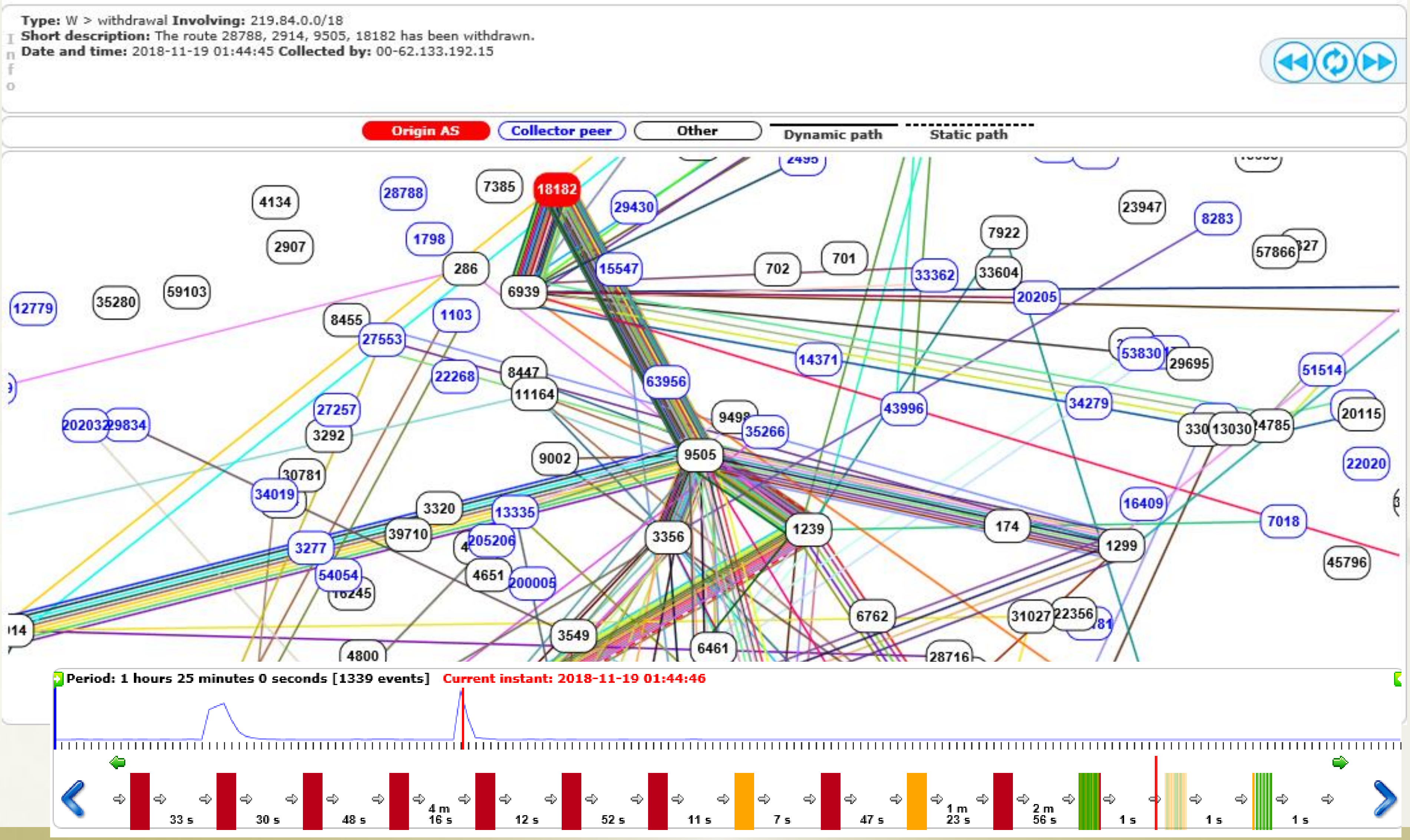


Type: A > pathchange **Involving:** 219.84.0.0/18
Short description: The route 12859 3257 1239 9505 18182 is changed to 12859 2914 2914 2914 2914 9505 18182
Path: 12859, 2914, 9505, 18182,
Date and time: 2018-11-19 01:39:32 **Collected by:** 00-213.136.1.132

98% prefixes disappear

Period: 1 hours 25 minutes 0 seconds [1339 events] Current instant: 2018-11-19 01:39:39

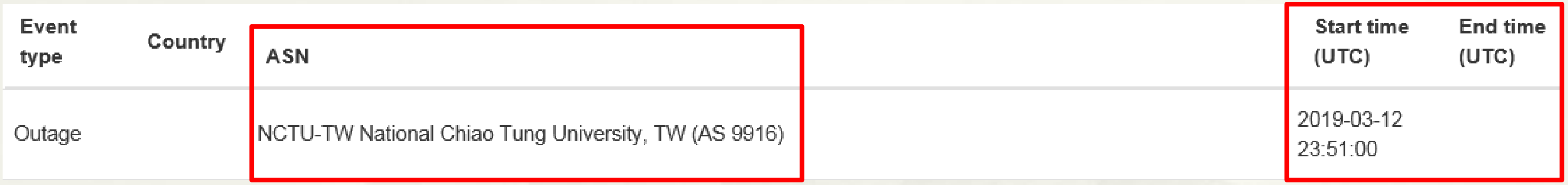
ASN 18182
Recovery from BGP Outage



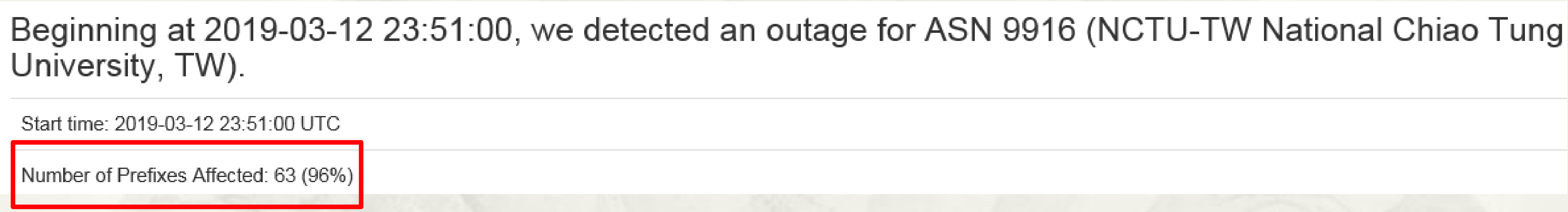
Type: W > withdrawal **Involving:** 219.84.0.0/18
Short description: The route 28788, 2914, 9505, 18182 has been withdrawn.
Date and time: 2018-11-19 01:44:45 **Collected by:** 00-62.133.192.15

Period: 1 hours 25 minutes 0 seconds [1339 events] Current instant: 2018-11-19 01:44:46

BGP Outage
ASN 9916 (NCTU)



Event type	Country	ASN	Start time (UTC)	End time (UTC)
Outage		NCTU-TW National Chiao Tung University, TW (AS 9916)	2019-03-12 23:51:00	



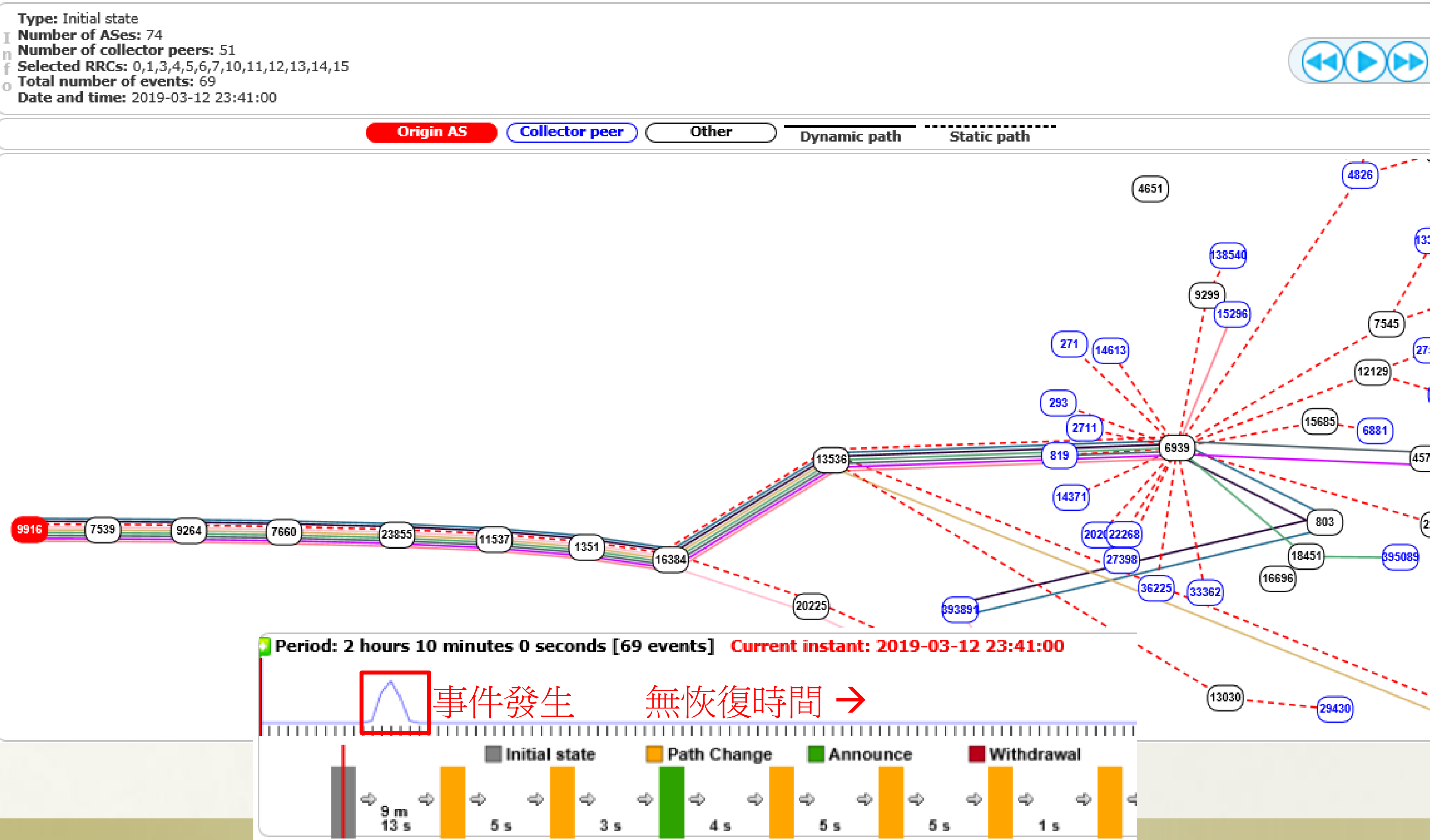
Beginning at 2019-03-12 23:51:00, we detected an outage for ASN 9916 (NCTU-TW National Chiao Tung University, TW).

Start time: 2019-03-12 23:51:00 UTC

Number of Prefixes Affected: 63 (96%)

https://bgpstream.com/event/197956

ASN 9916 (NCTU)
Before BGP Outage

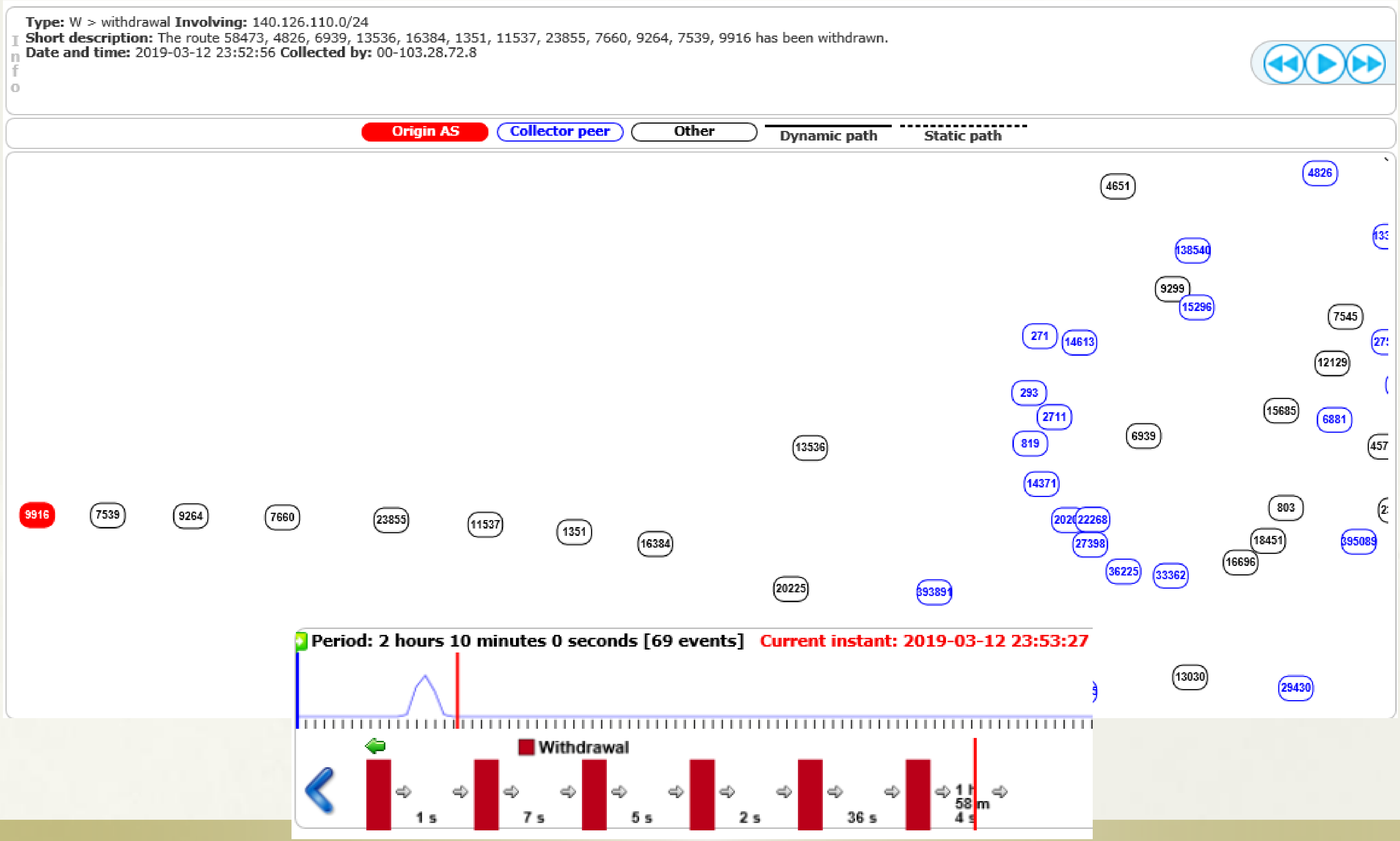


Type: Initial state
Number of ASes: 74
Number of collector peers: 51
Selected RRCs: 0,1,3,4,5,6,7,10,11,12,13,14,15
Total number of events: 69
Date and time: 2019-03-12 23:41:00

Period: 2 hours 10 minutes 0 seconds [69 events] **Current instant: 2019-03-12 23:41:00**

事件發生 無恢復時間 →

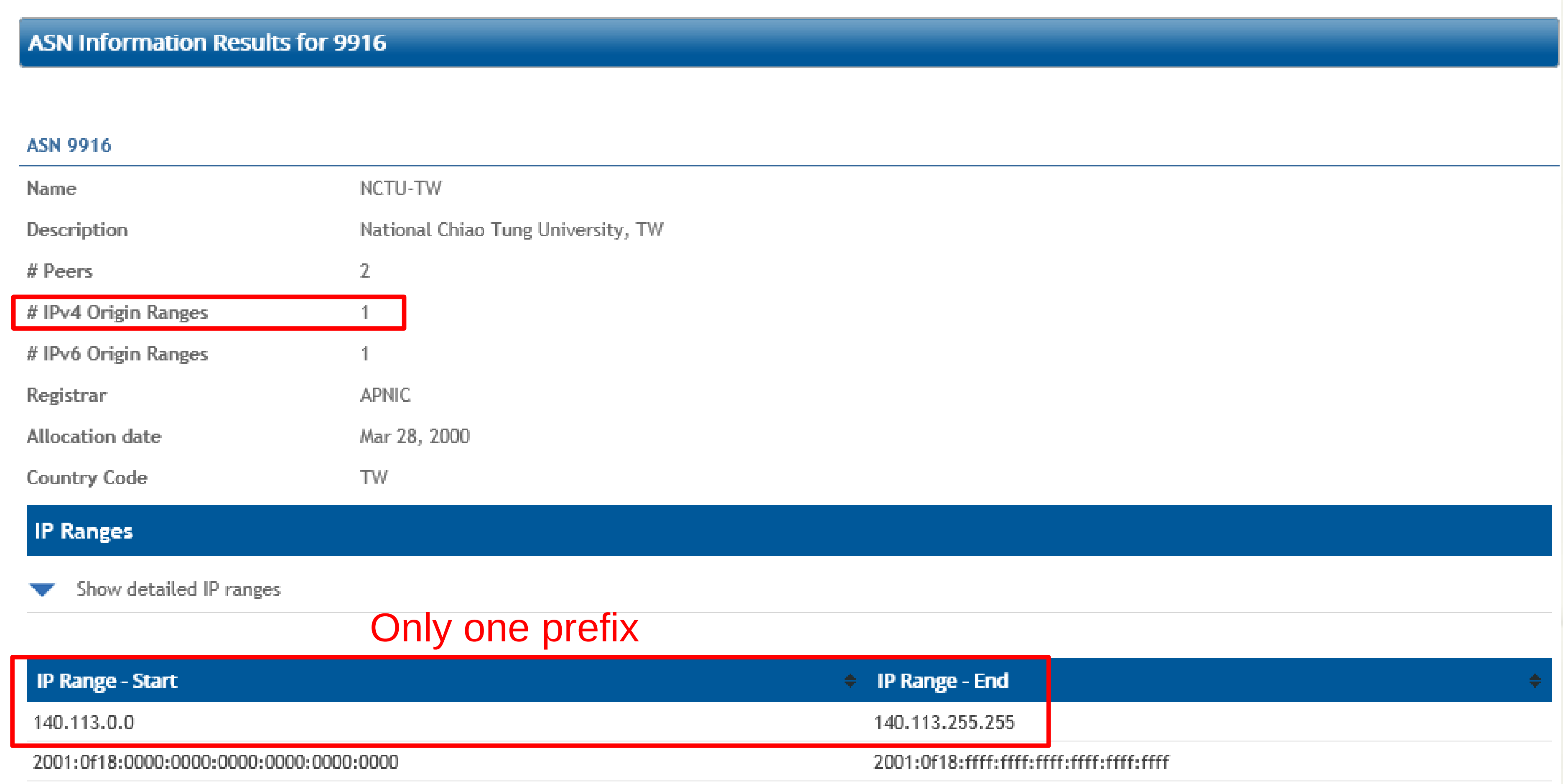
ASN 9916 (NCTU) BGP Outage



Type: W > withdrawal **Involving:** 140.126.110.0/24
Short description: The route 58473, 4826, 6939, 13536, 16384, 1351, 11537, 23855, 7660, 9264, 7539, 9916 has been withdrawn.
Date and time: 2019-03-12 23:52:56 **Collected by:** 00-103.28.72.8

Period: 2 hours 10 minutes 0 seconds [69 events] **Current instant: 2019-03-12 23:53:27**

Prefix for ASN 9916 from dnsstuff.com



ASN Information Results for 9916

ASN 9916

Name	NCTU-TW
Description	National Chiao Tung University, TW
# Peers	2
# IPv4 Origin Ranges	1
# IPv6 Origin Ranges	1
Registrar	APNIC
Allocation date	Mar 28, 2000
Country Code	TW

IP Ranges

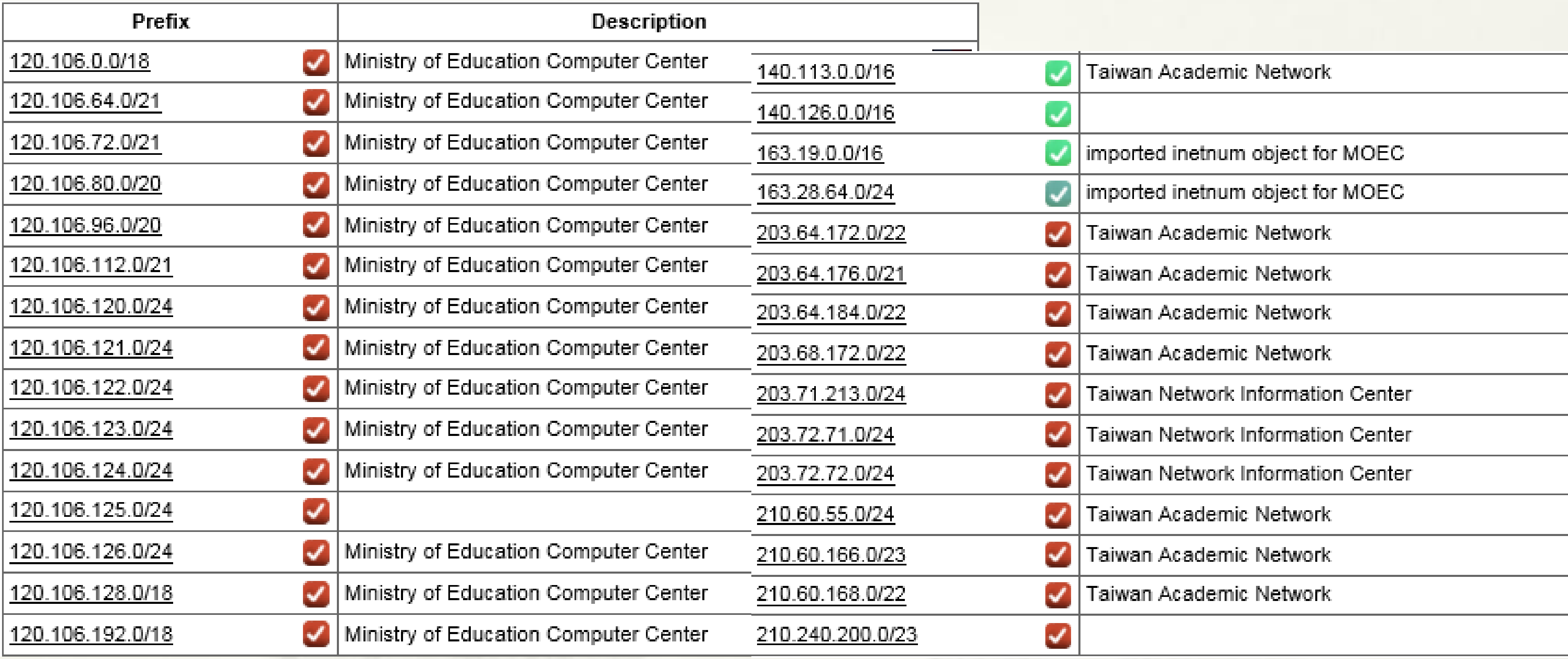
Show detailed IP ranges

Only one prefix

IP Range - Start	IP Range - End
140.113.0.0	140.113.255.255
2001:0f18:0000:0000:0000:0000:0000:0000	2001:0f18:ffff:ffff:ffff:ffff:ffff:ffff

https://tools.dnsstuff.com/#asnInformation|type=asn&&value=9916

Prefix for ASN 9916 from he.net



Prefix		Description
120.106.0.0/18	✓	Ministry of Education Computer Center
120.106.64.0/21	✓	Ministry of Education Computer Center
120.106.72.0/21	✓	Ministry of Education Computer Center
120.106.80.0/20	✓	Ministry of Education Computer Center
120.106.96.0/20	✓	Ministry of Education Computer Center
120.106.112.0/21	✓	Ministry of Education Computer Center
120.106.120.0/24	✓	Ministry of Education Computer Center
120.106.121.0/24	✓	Ministry of Education Computer Center
120.106.122.0/24	✓	Ministry of Education Computer Center
120.106.123.0/24	✓	Ministry of Education Computer Center
120.106.124.0/24	✓	Ministry of Education Computer Center
120.106.125.0/24	✓	
120.106.126.0/24	✓	Ministry of Education Computer Center
120.106.128.0/18	✓	Ministry of Education Computer Center
120.106.192.0/18	✓	Ministry of Education Computer Center

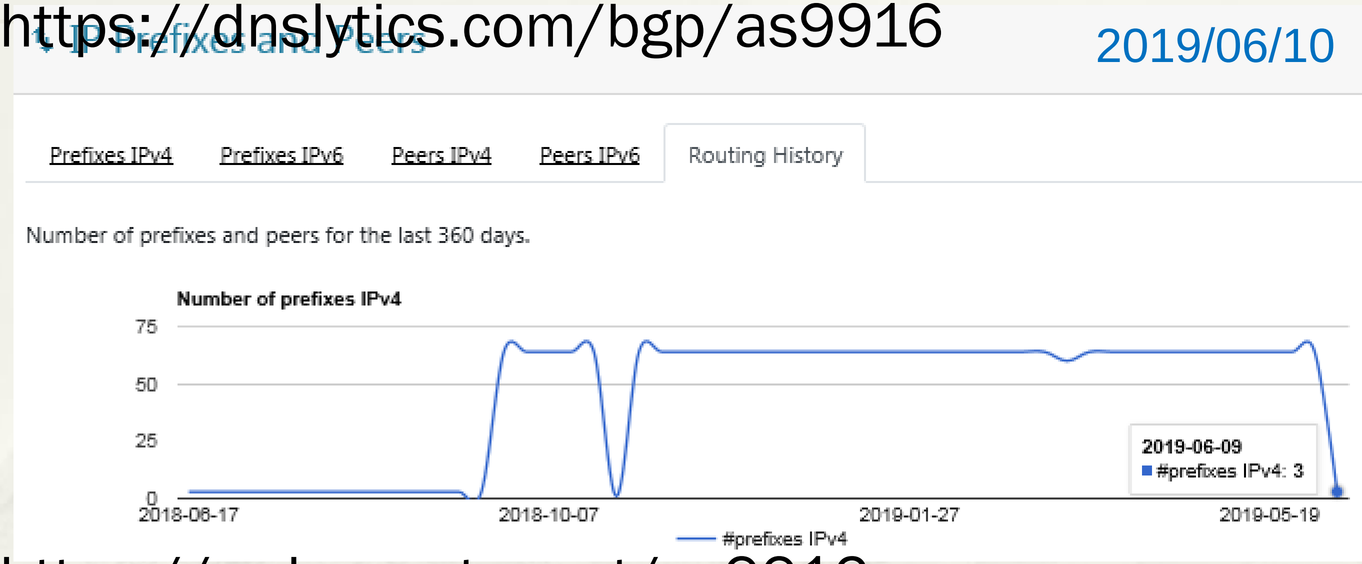
140.113.0.0/16	✓	Taiwan Academic Network
140.126.0.0/16	✓	
163.19.0.0/16	✓	imported inetnum object for MOEC
163.28.64.0/24	✓	imported inetnum object for MOEC
203.64.172.0/22	✓	Taiwan Academic Network
203.64.176.0/21	✓	Taiwan Academic Network
203.64.184.0/22	✓	Taiwan Academic Network
203.68.172.0/22	✓	Taiwan Academic Network
203.71.213.0/24	✓	Taiwan Network Information Center
203.72.71.0/24	✓	Taiwan Network Information Center
203.72.72.0/24	✓	Taiwan Network Information Center
210.60.55.0/24	✓	Taiwan Academic Network
210.60.166.0/23	✓	Taiwan Academic Network
210.60.168.0/22	✓	Taiwan Academic Network
210.240.200.0/23	✓	

2019/06/10
https://bgp.he.net/AS9916#_prefixes

Number of prefixes History

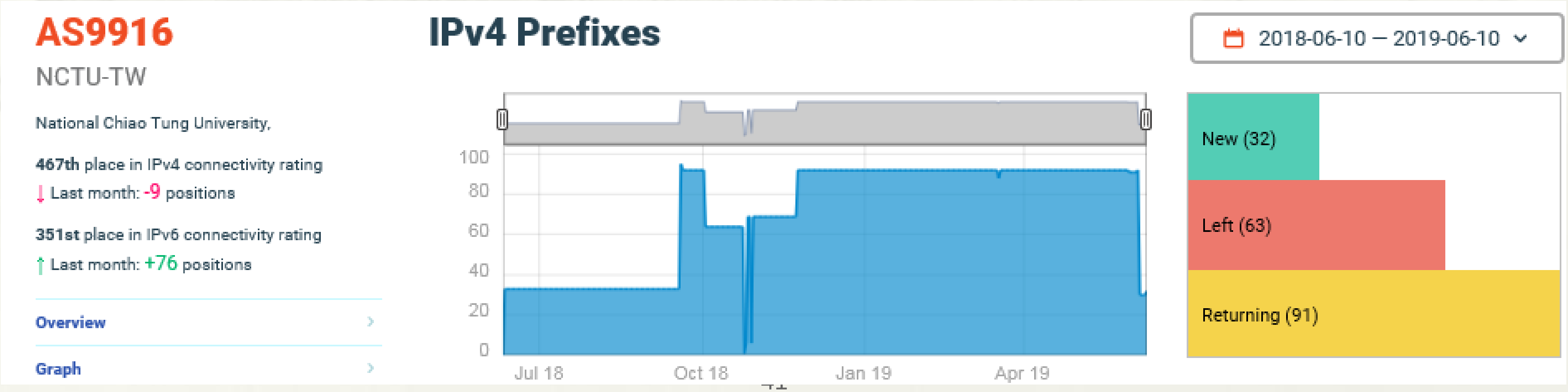
- https://dnslytics.com/bgp/as9916

2019/06/10



Number of prefixes and peers for the last 360 days.

- https://radar.qrator.net/as9916



AS9916

NCTU-TW

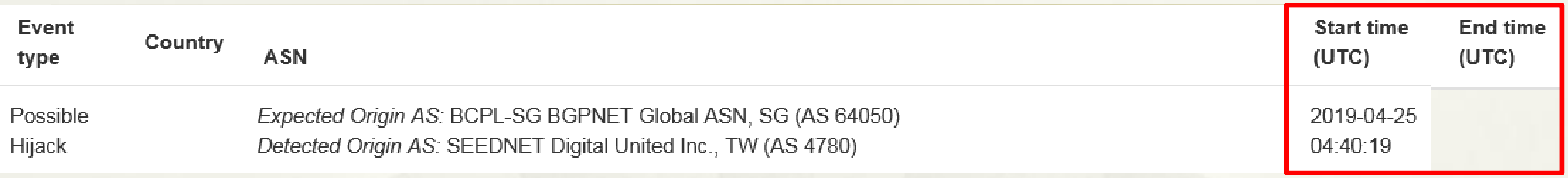
National Chiao Tung University,

467th place in IPv4 connectivity rating
↓ Last month: -9 positions

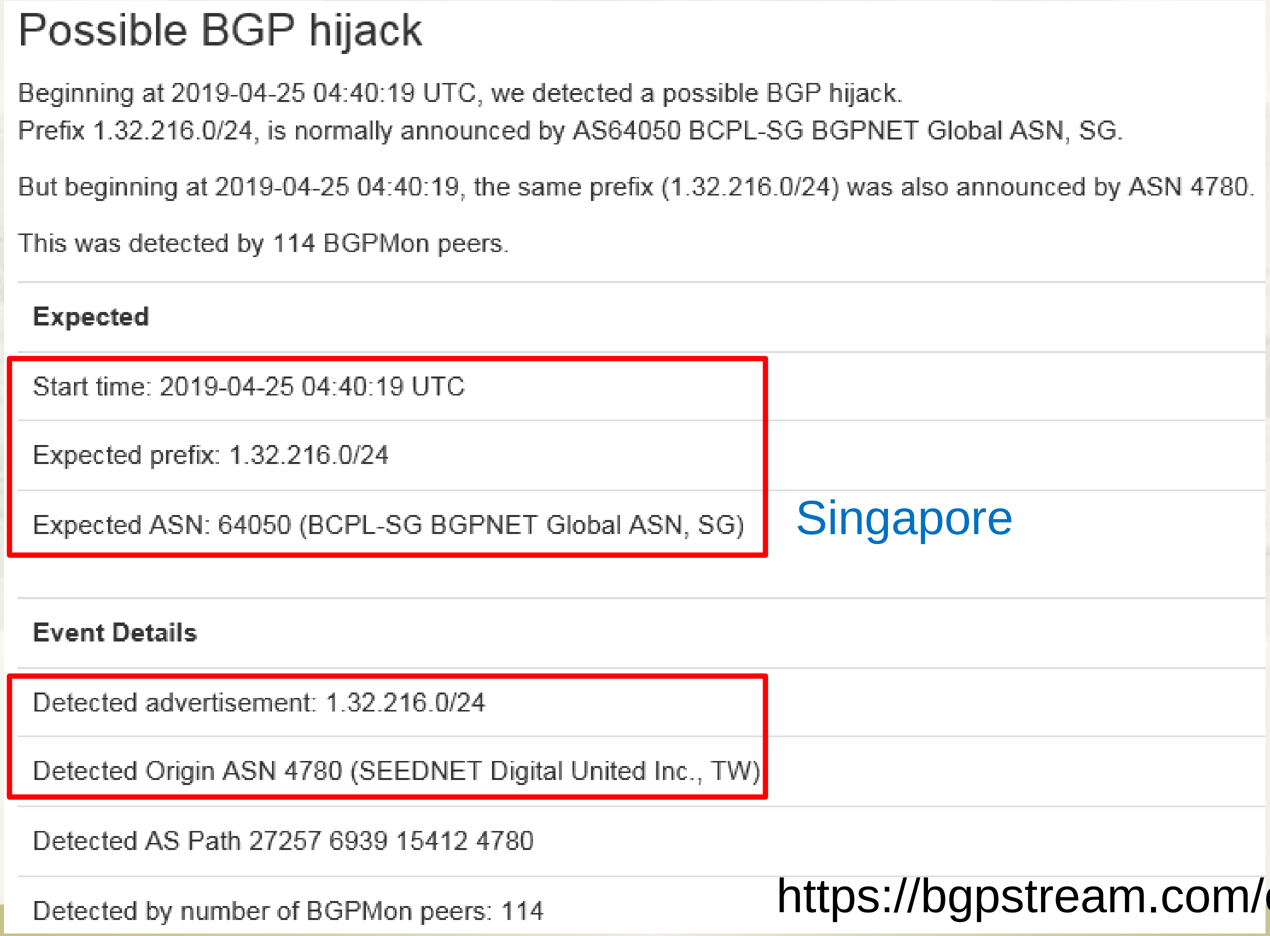
351st place in IPv6 connectivity rating
↑ Last month: +76 positions

Partial BGP Hijacking
The same prefix

Partial BGP Hijack
The same prefix



Event type	Country	ASN	Start time (UTC)	End time (UTC)
Possible Hijack		*Expected Origin AS:* BCPL-SG BGPNET Global ASN, SG (AS 64050) *Detected Origin AS:* SEEDNET Digital United Inc., TW (AS 4780)	2019-04-25 04:40:19	



Possible BGP hijack

Beginning at 2019-04-25 04:40:19 UTC, we detected a possible BGP hijack.
Prefix 1.32.216.0/24, is normally announced by AS64050 BCPL-SG BGPNET Global ASN, SG.

But beginning at 2019-04-25 04:40:19, the same prefix (1.32.216.0/24) was also announced by ASN 4780.

This was detected by 114 BGPMon peers.

Expected

Start time: 2019-04-25 04:40:19 UTC

Expected prefix: 1.32.216.0/24

Expected ASN: 64050 (BCPL-SG BGPNET Global ASN, SG)

Singapore

Event Details

Detected advertisement: 1.32.216.0/24

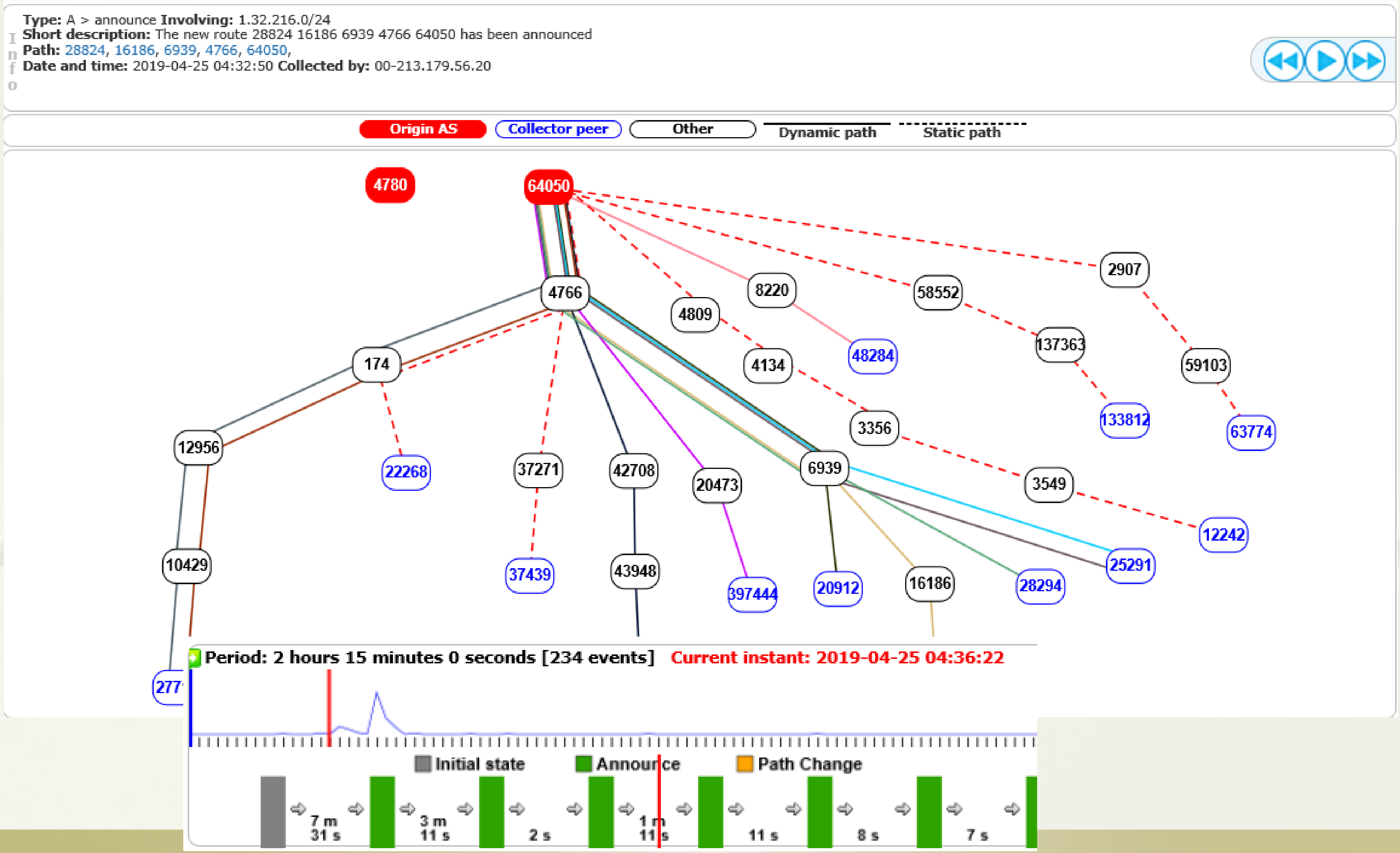
Detected Origin ASN 4780 (SEEDNET Digital United Inc., TW)

Detected AS Path 27257 6939 15412 4780

Detected by number of BGPMon peers: 114

https://bgpstream.com/event/202043

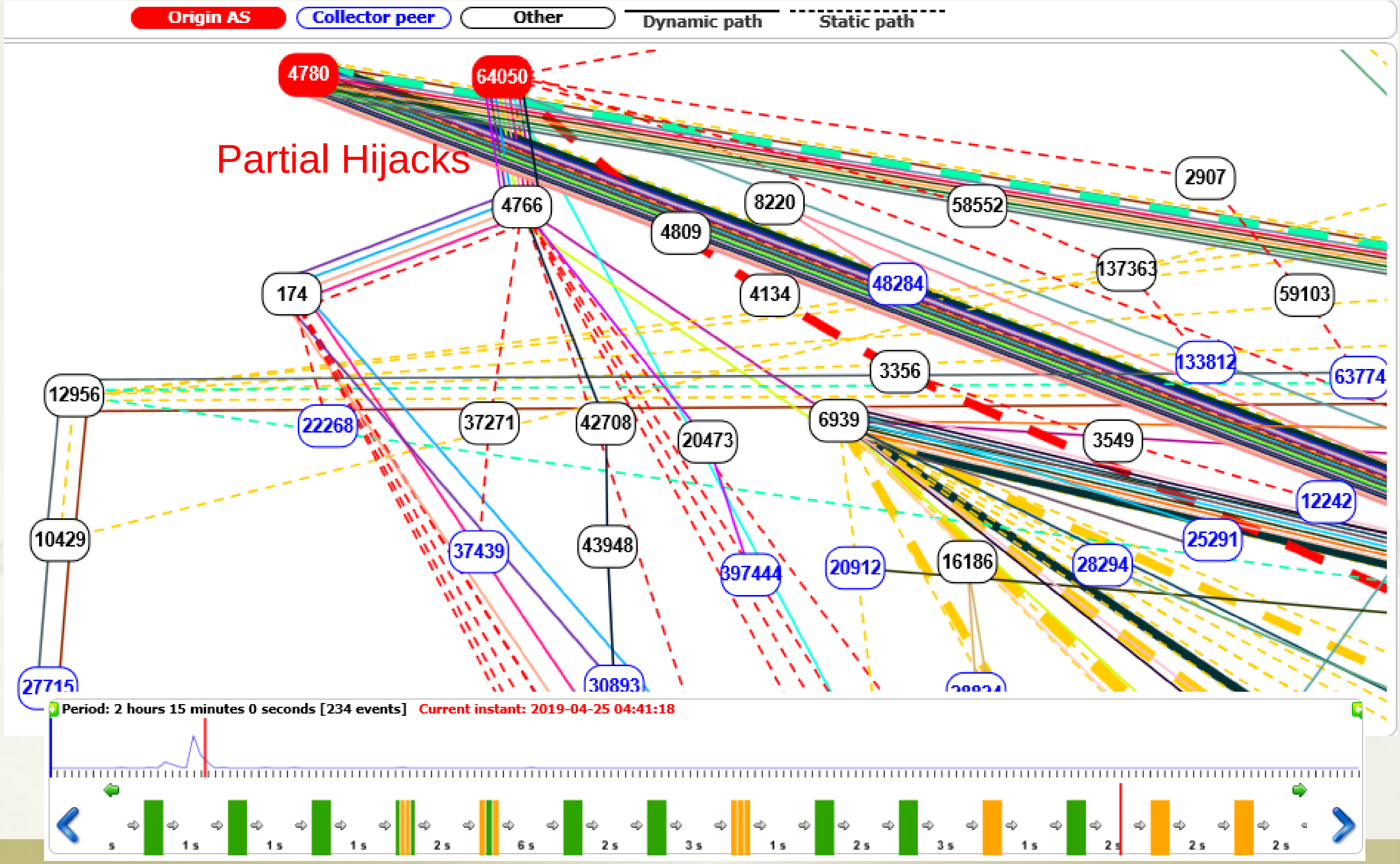
1.32.216.0/24
Before Hijacks



Type: A > announce **Involving:** 1.32.216.0/24
Short description: The new route 28824 16186 6939 4766 64050 has been announced
Path: 28824, 16186, 6939, 4766, 64050,
Date and time: 2019-04-25 04:32:50 **Collected by:** 00-213.179.56.20

Period: 2 hours 15 minutes 0 seconds [234 events] **Current instant: 2019-04-25 04:36:22**

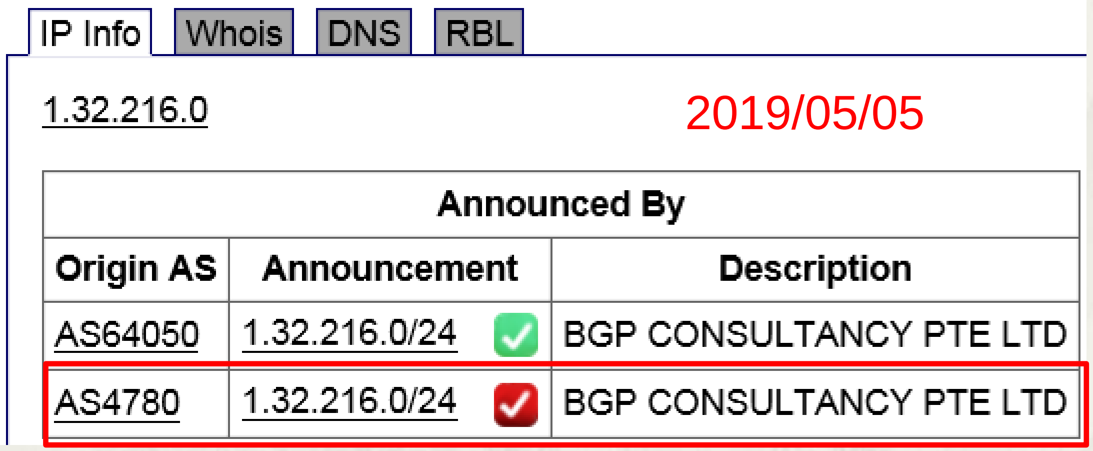
1.32.216.0/24 Hijacks



Period: 2 hours 15 minutes 0 seconds [234 events] Current instant: 2019-04-25 04:41:18

1.32.216.0/24
Query from other looking glass

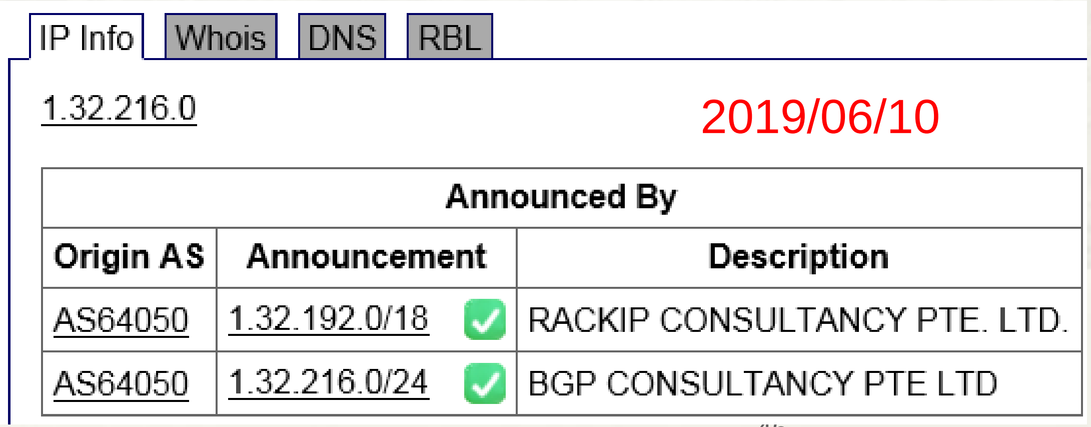
- https://bgp.he.net/ip/1.32.216.0



1.32.216.0

2019/05/05

Announced By		
Origin AS	**Announcement**	**Description**
AS64050	1.32.216.0/24 ✓	BGP CONSULTANCY PTE LTD
AS4780	1.32.216.0/24 ✓	BGP CONSULTANCY PTE LTD



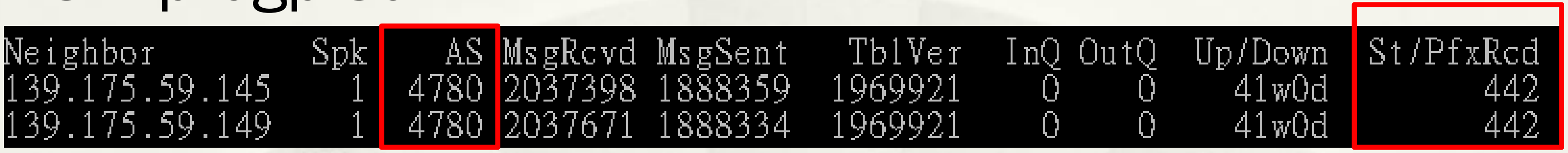
1.32.216.0

2019/06/10

Announced By		
Origin AS	**Announcement**	**Description**
AS64050	1.32.192.0/18 ✓	RACKIP CONSULTANCY PTE. LTD.
AS64050	1.32.216.0/24 ✓	BGP CONSULTANCY PTE LTD

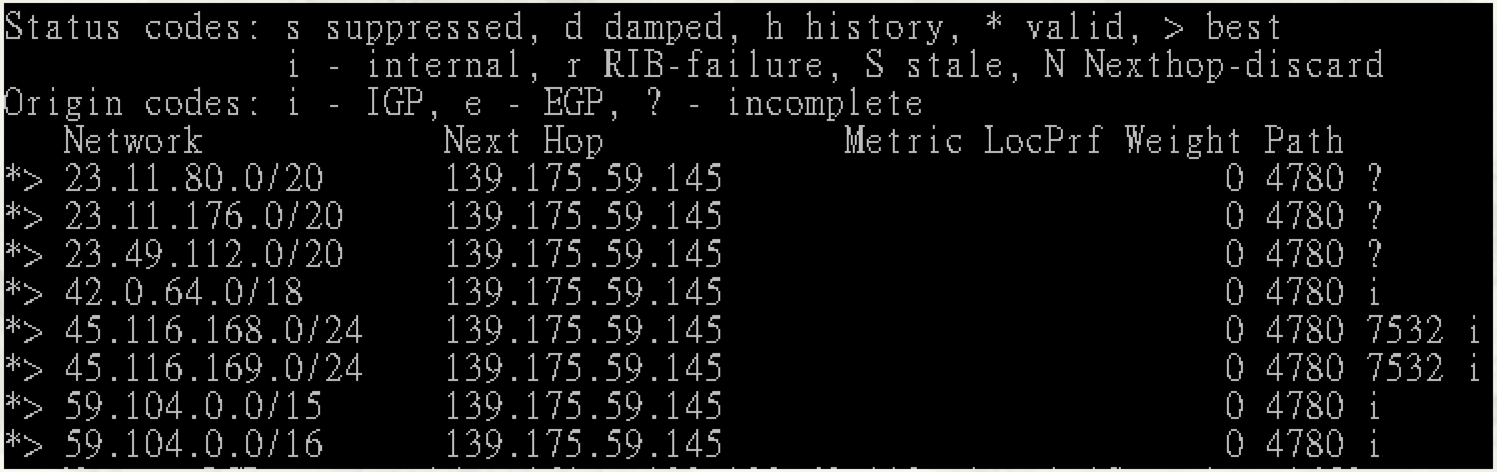
BGP Hijack: 1.32.216.0/24 Query from NTU

- sh ip bgp sum



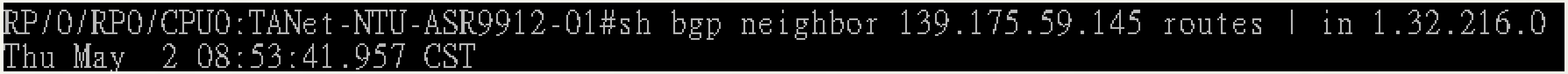
```
Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
139.175.59.145    1  4780 2037398 1888359  1969921    0    0    41w0d        442
139.175.59.149    1  4780 2037671 1888334  1969921    0    0    41w0d        442
```

- sh bgp neighbor 139.175.59.145 routes



```
Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            Next Hop            Metric LocPrf Weight Path
*> 23.11.80.0/20      139.175.59.145                       0 4780 ?
*> 23.11.176.0/20     139.175.59.145                       0 4780 ?
*> 23.49.112.0/20     139.175.59.145                       0 4780 ?
*> 42.0.64.0/18       139.175.59.145                       0 4780 i
*> 45.116.168.0/24    139.175.59.145                       0 4780 7532 i
*> 45.116.169.0/24    139.175.59.145                       0 4780 7532 i
*> 59.104.0.0/15      139.175.59.145                       0 4780 i
*> 59.104.0.0/16      139.175.59.145                       0 4780 i
```

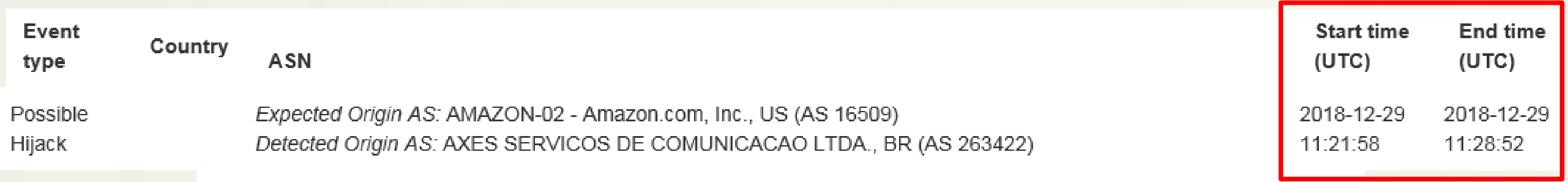
- 未發現此筆 Route



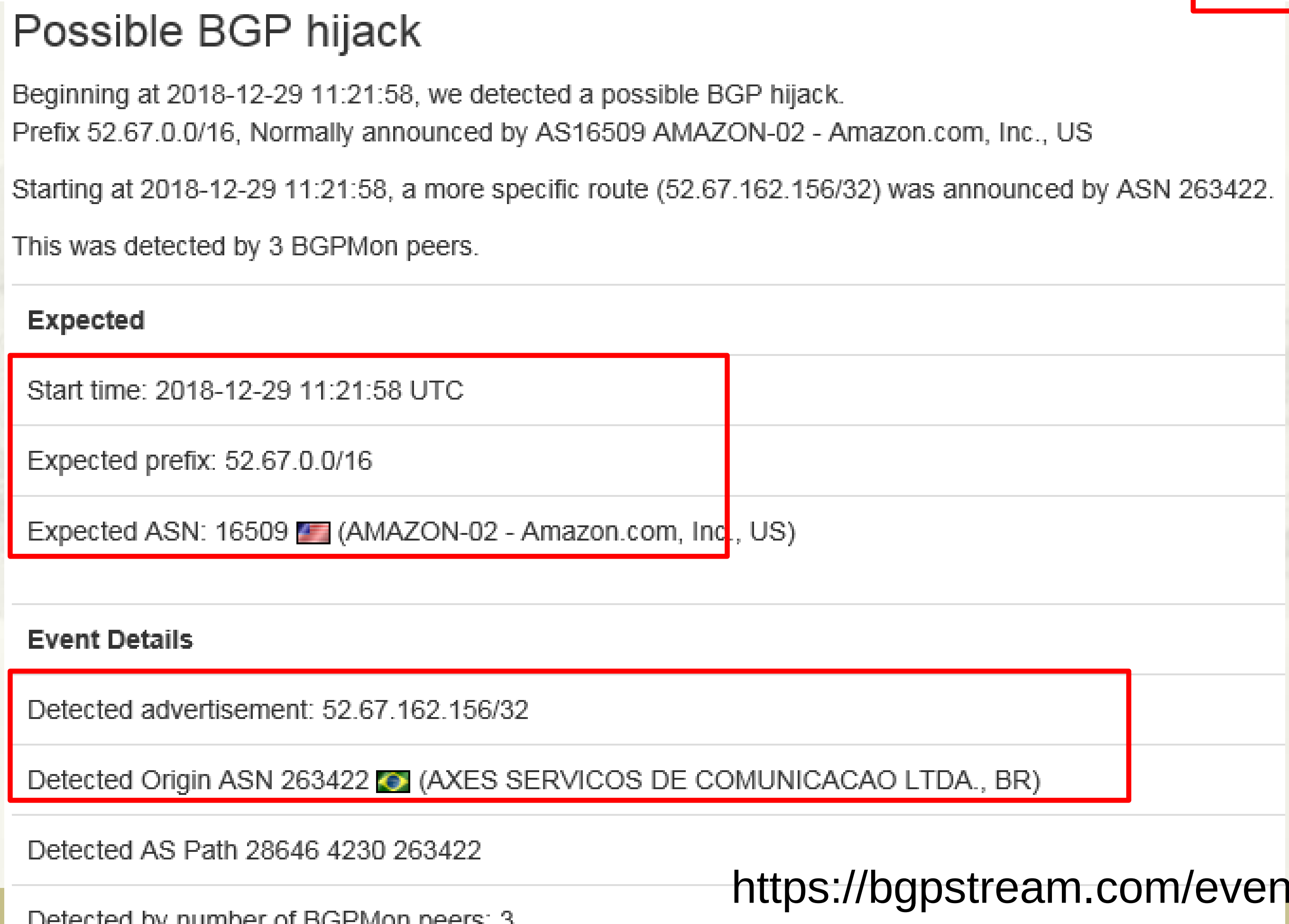
```
RP/0/RP0/CPU0:TANet-NTU-ASR9912-01#sh bgp neighbor 139.175.59.145 routes | in 1.32.216.0
Thu May  2 08:53:41.957 CST
```

Complete BGP Hijacking a more specific route

Complete BGP Hijack
a more specific route from AS 263422



Event type	Country	ASN	Start time (UTC)	End time (UTC)
Possible Hijack		*Expected Origin AS:* AMAZON-02 - Amazon.com, Inc., US (AS 16509) *Detected Origin AS:* AXES SERVICOS DE COMUNICACAO LTDA., BR (AS 263422)	2018-12-29 11:21:58	2018-12-29 11:28:52



Possible BGP hijack

Beginning at 2018-12-29 11:21:58, we detected a possible BGP hijack.
Prefix 52.67.0.0/16, Normally announced by AS16509 AMAZON-02 - Amazon.com, Inc., US

Starting at 2018-12-29 11:21:58, a more specific route (52.67.162.156/32) was announced by ASN 263422.

This was detected by 3 BGPMon peers.

Expected

Start time: 2018-12-29 11:21:58 UTC

Expected prefix: 52.67.0.0/16

Expected ASN: 16509 🇺🇸 (AMAZON-02 - Amazon.com, Inc., US)

Event Details

Detected advertisement: 52.67.162.156/32

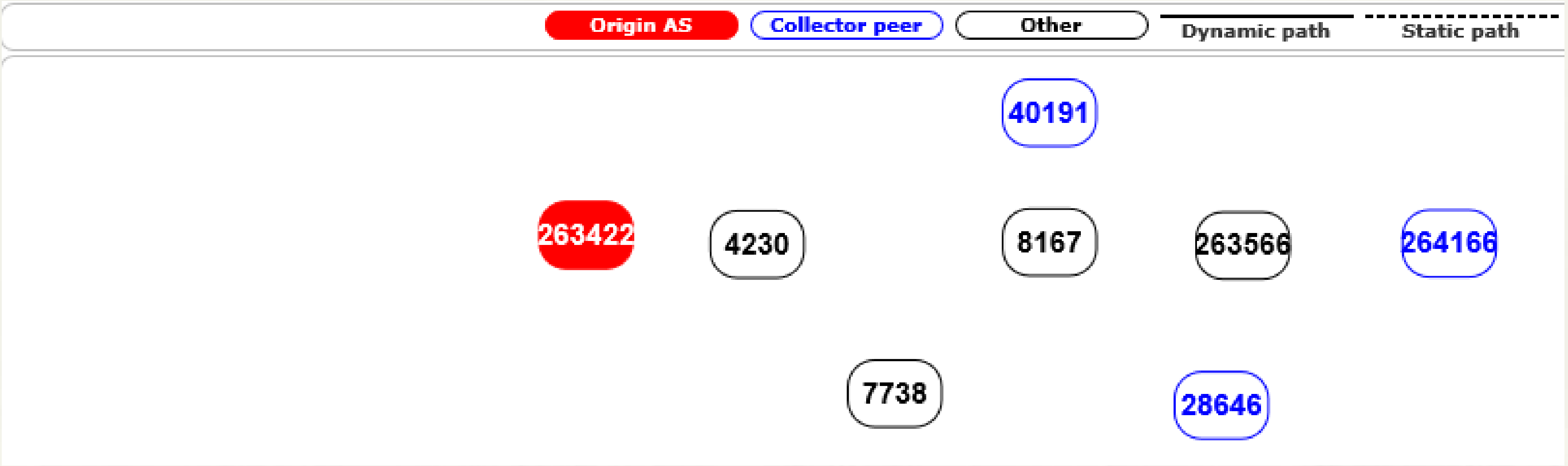
Detected Origin ASN 263422 🇧🇷 (AXES SERVICOS DE COMUNICACAO LTDA., BR)

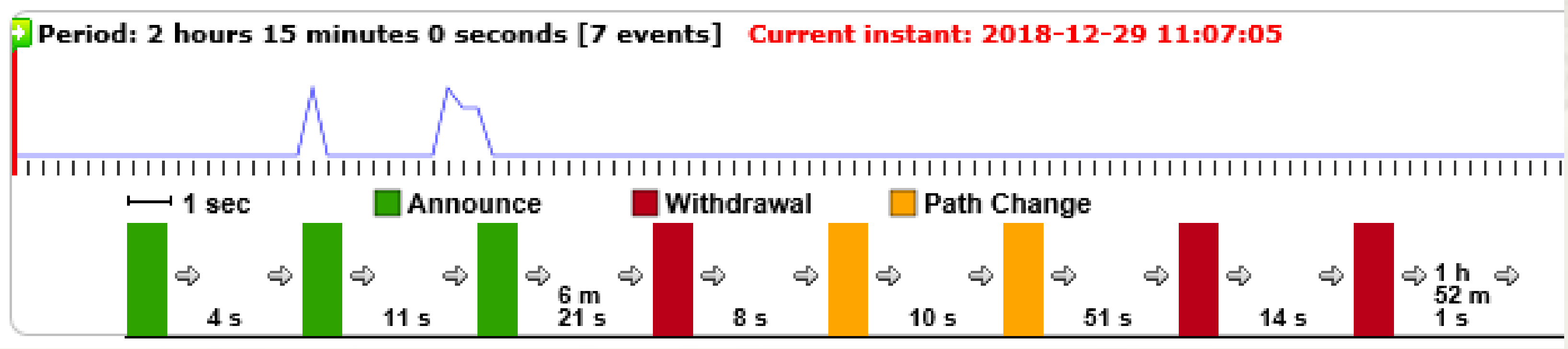
Detected AS Path 28646 4230 263422

Detected by number of BGPMon peers: 3

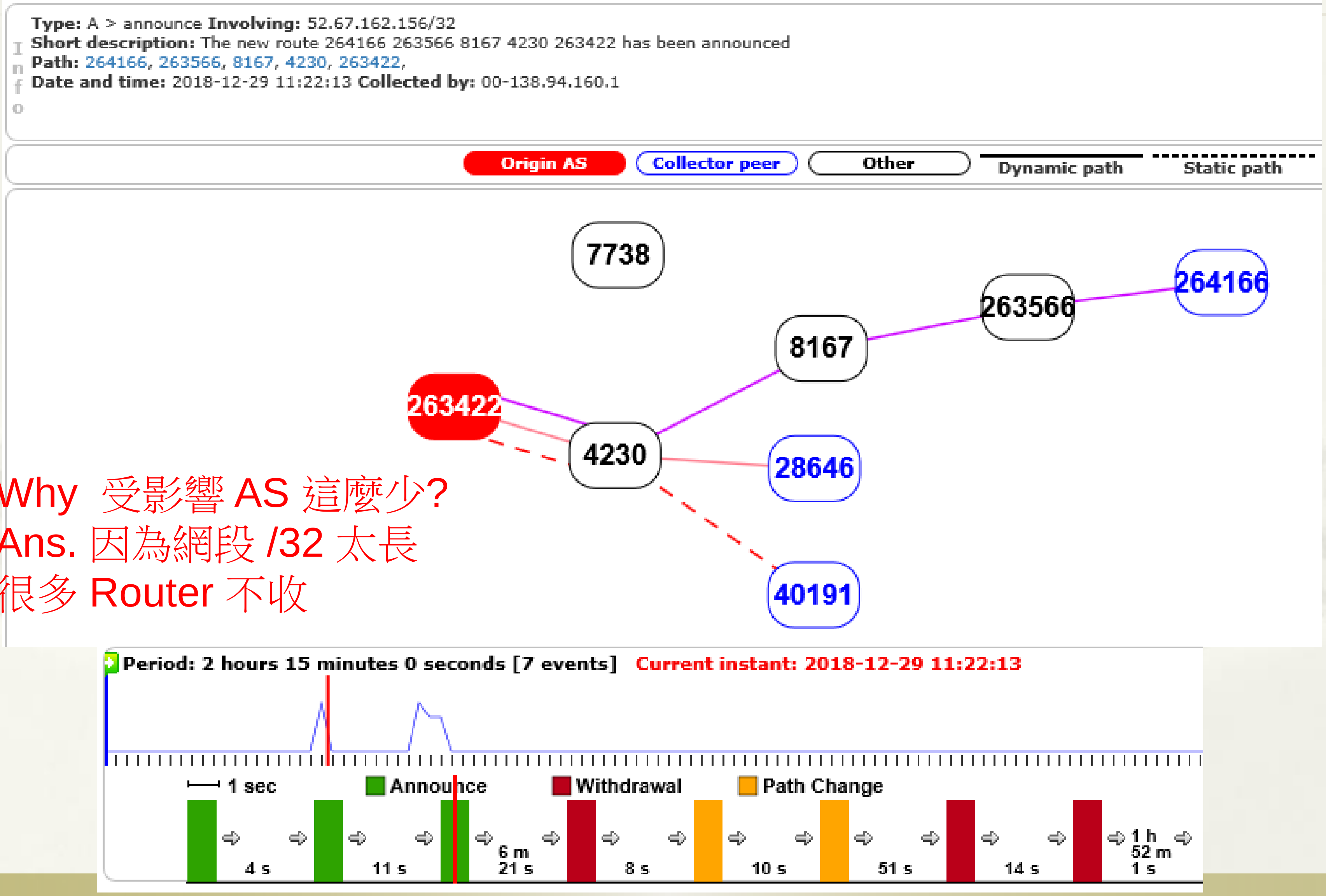
https://bgpstream.com/event/172435

52.67.162.156/32
Before Hijack




Period: 2 hours 15 minutes 0 seconds [7 events] Current instant: 2018-12-29 11:07:05

52.67.162.156/32 Hijacks

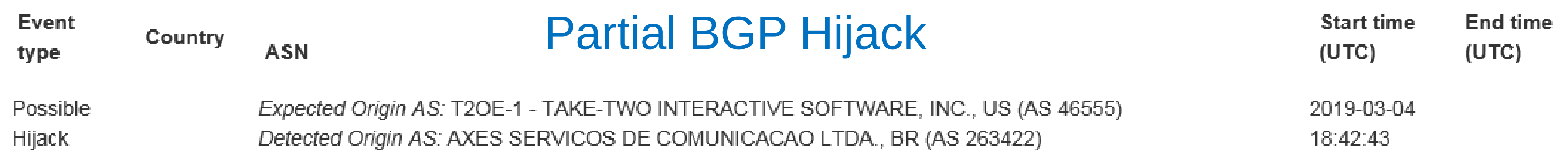


Type: A > announce **Involving:** 52.67.162.156/32
Short description: The new route 264166 263566 8167 4230 263422 has been announced
Path: 264166, 263566, 8167, 4230, 263422,
Date and time: 2018-12-29 11:22:13 **Collected by:** 00-138.94.160.1

Period: 2 hours 15 minutes 0 seconds [7 events] **Current instant: 2018-12-29 11:22:13**

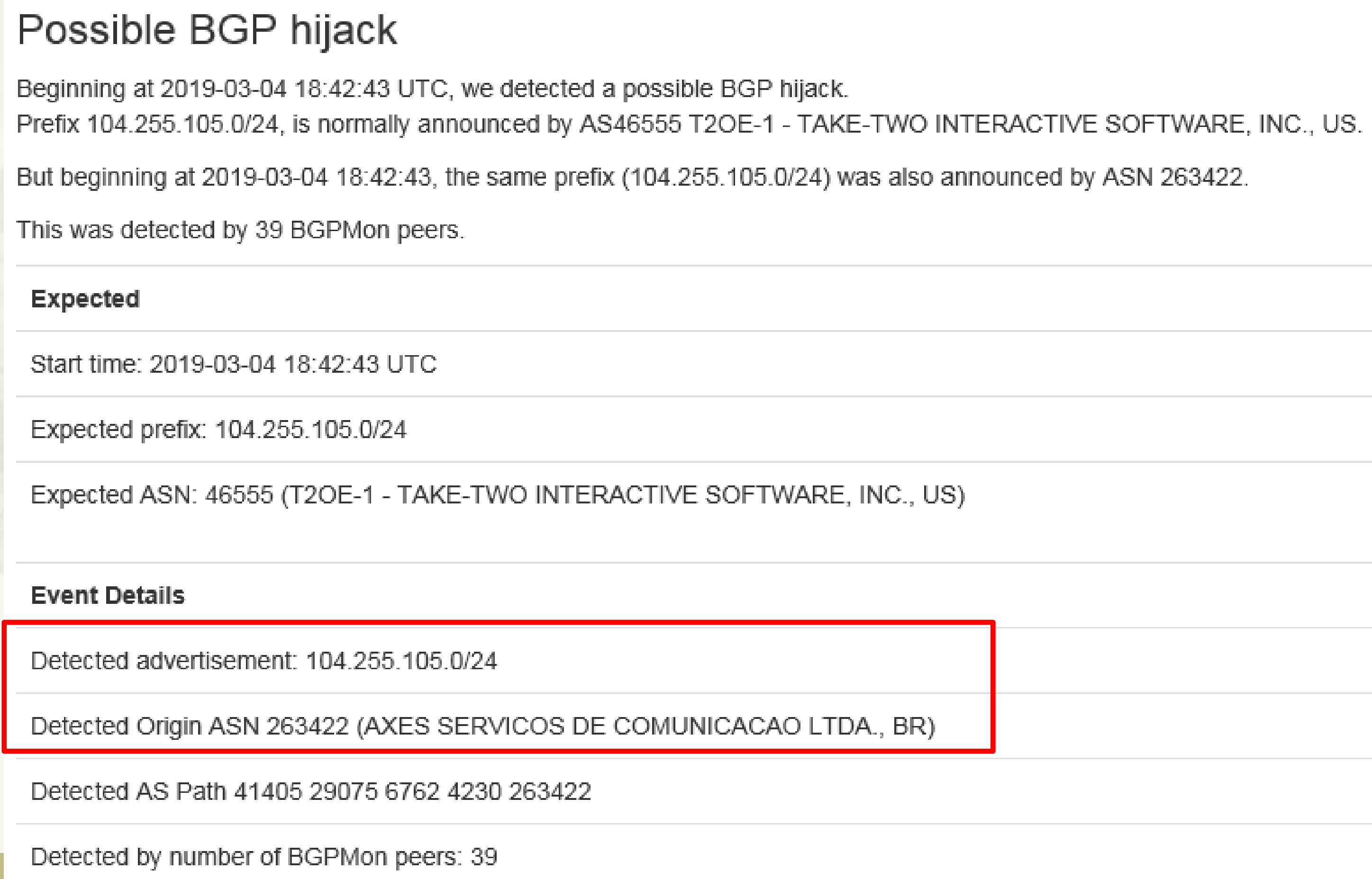
Why 受影響 AS 這麼少?
Ans. 因為網段 /32 太長
很多 Router 不收

相同 AS 263422
不同網段 /32 /24 受影響之 AS



Partial BGP Hijack

Event type	Country	ASN	Start time (UTC)	End time (UTC)
Possible Hijack		*Expected Origin AS:* T2OE-1 - TAKE-TWO INTERACTIVE SOFTWARE, INC., US (AS 46555) *Detected Origin AS:* AXES SERVICOS DE COMUNICACAO LTDA., BR (AS 263422)	2019-03-04 18:42:43	



Possible BGP hijack

Beginning at 2019-03-04 18:42:43 UTC, we detected a possible BGP hijack.
Prefix 104.255.105.0/24, is normally announced by AS46555 T2OE-1 - TAKE-TWO INTERACTIVE SOFTWARE, INC., US.

But beginning at 2019-03-04 18:42:43, the same prefix (104.255.105.0/24) was also announced by ASN 263422.

This was detected by 39 BGPMon peers.

Expected

Start time: 2019-03-04 18:42:43 UTC

Expected prefix: 104.255.105.0/24

Expected ASN: 46555 (T2OE-1 - TAKE-TWO INTERACTIVE SOFTWARE, INC., US)

Event Details

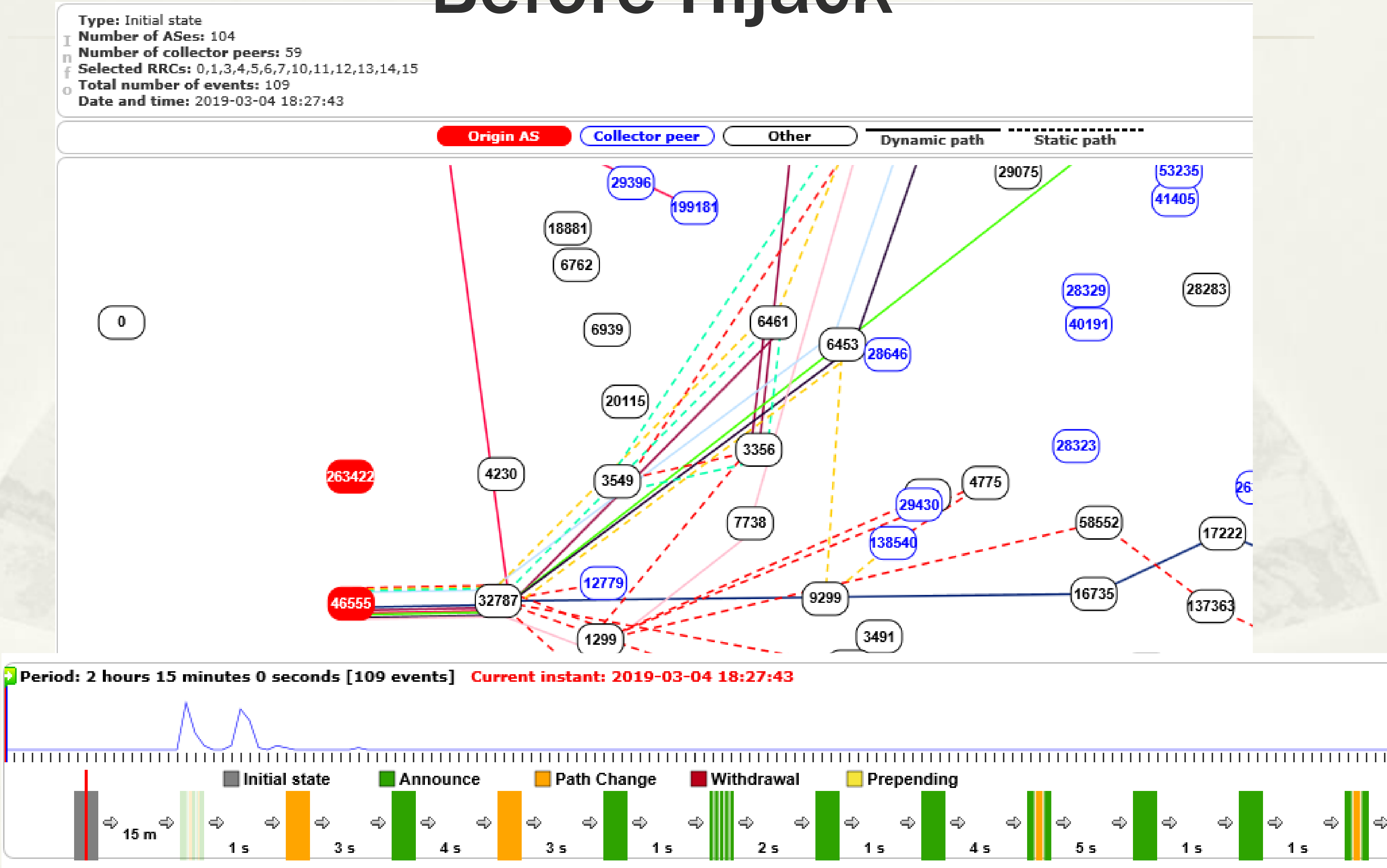
Detected advertisement: 104.255.105.0/24

Detected Origin ASN 263422 (AXES SERVICOS DE COMUNICACAO LTDA., BR)

Detected AS Path 41405 29075 6762 4230 263422

Detected by number of BGPMon peers: 39

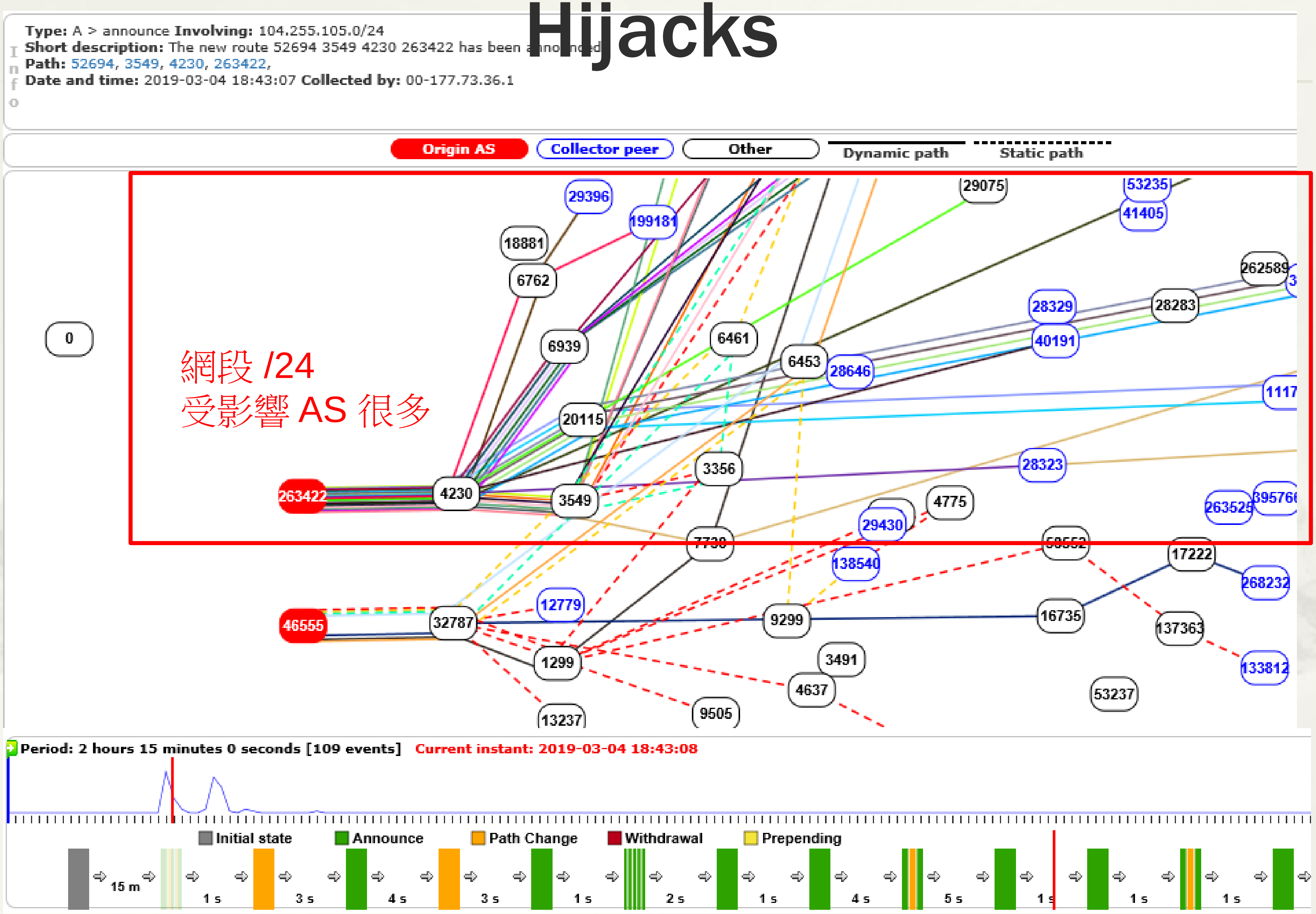
104.255.105.0/24
Before Hijack



Type: Initial state
Number of ASes: 104
Number of collector peers: 59
Selected RRCs: 0,1,3,4,5,6,7,10,11,12,13,14,15
Total number of events: 109
Date and time: 2019-03-04 18:27:43

Period: 2 hours 15 minutes 0 seconds [109 events] Current instant: 2019-03-04 18:27:43

104.255.105.0/24 Hijacks



Type: A > announce **Involving:** 104.255.105.0/24
Short description: The new route 52694 3549 4230 263422 has been announced
Path: 52694, 3549, 4230, 263422,
Date and time: 2019-03-04 18:43:07 **Collected by:** 00-177.73.36.1

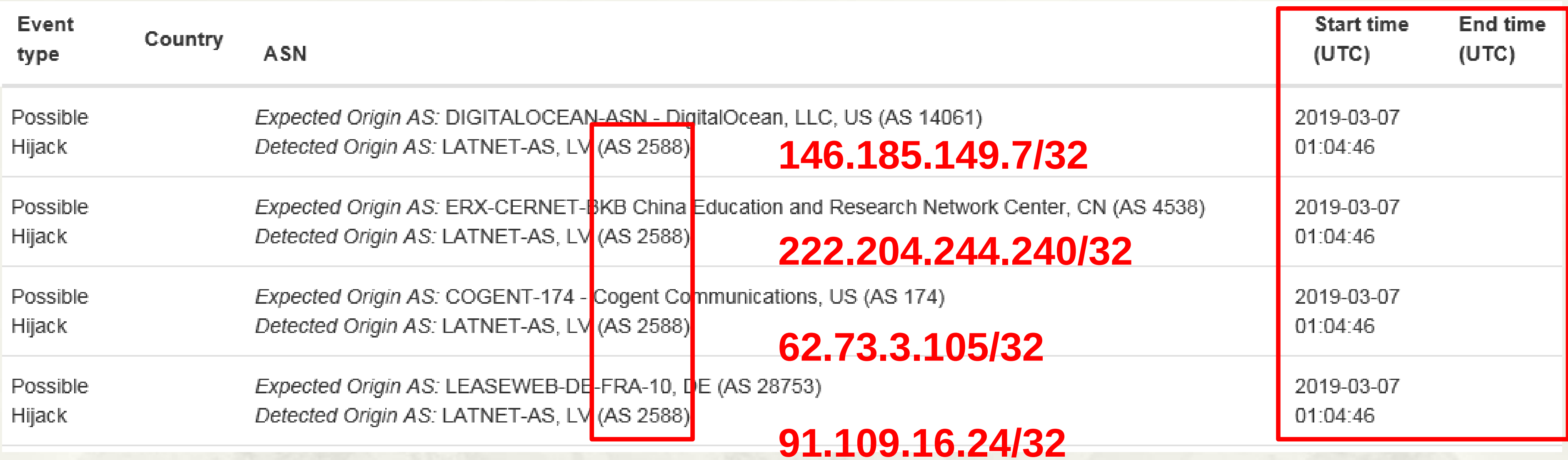
Origin AS | Collector peer | Other | Dynamic path | Static path

網段 /24
受影響 AS 很多

Period: 2 hours 15 minutes 0 seconds [109 events] **Current instant: 2019-03-04 18:43:08**

🟫 Initial state 🟩 Announce 🟧 Path Change 🟥 Withdrawal 🟨 Prepending

BGP Hijacks by AS 2588



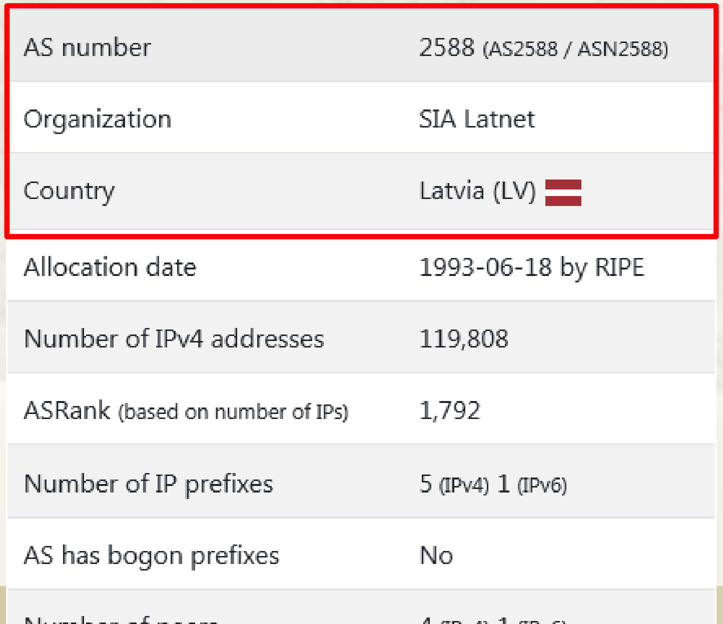
Event type	Country	ASN	Start time (UTC)	End time (UTC)
Possible Hijack		*Expected Origin AS:* DIGITALOCEAN-ASN - DigitalOcean, LLC, US (AS 14061) *Detected Origin AS:* LATNET-AS, LV (AS 2588)	2019-03-07 01:04:46	
Possible Hijack		*Expected Origin AS:* ERX-CERNET-BKB China Education and Research Network Center, CN (AS 4538) *Detected Origin AS:* LATNET-AS, LV (AS 2588)	2019-03-07 01:04:46	
Possible Hijack		*Expected Origin AS:* COGENT-174 - Cogent Communications, US (AS 174) *Detected Origin AS:* LATNET-AS, LV (AS 2588)	2019-03-07 01:04:46	
Possible Hijack		*Expected Origin AS:* LEASEWEB-DE-FRA-10, DE (AS 28753) *Detected Origin AS:* LATNET-AS, LV (AS 2588)	2019-03-07 01:04:46	

146.185.149.7/32

222.204.244.240/32

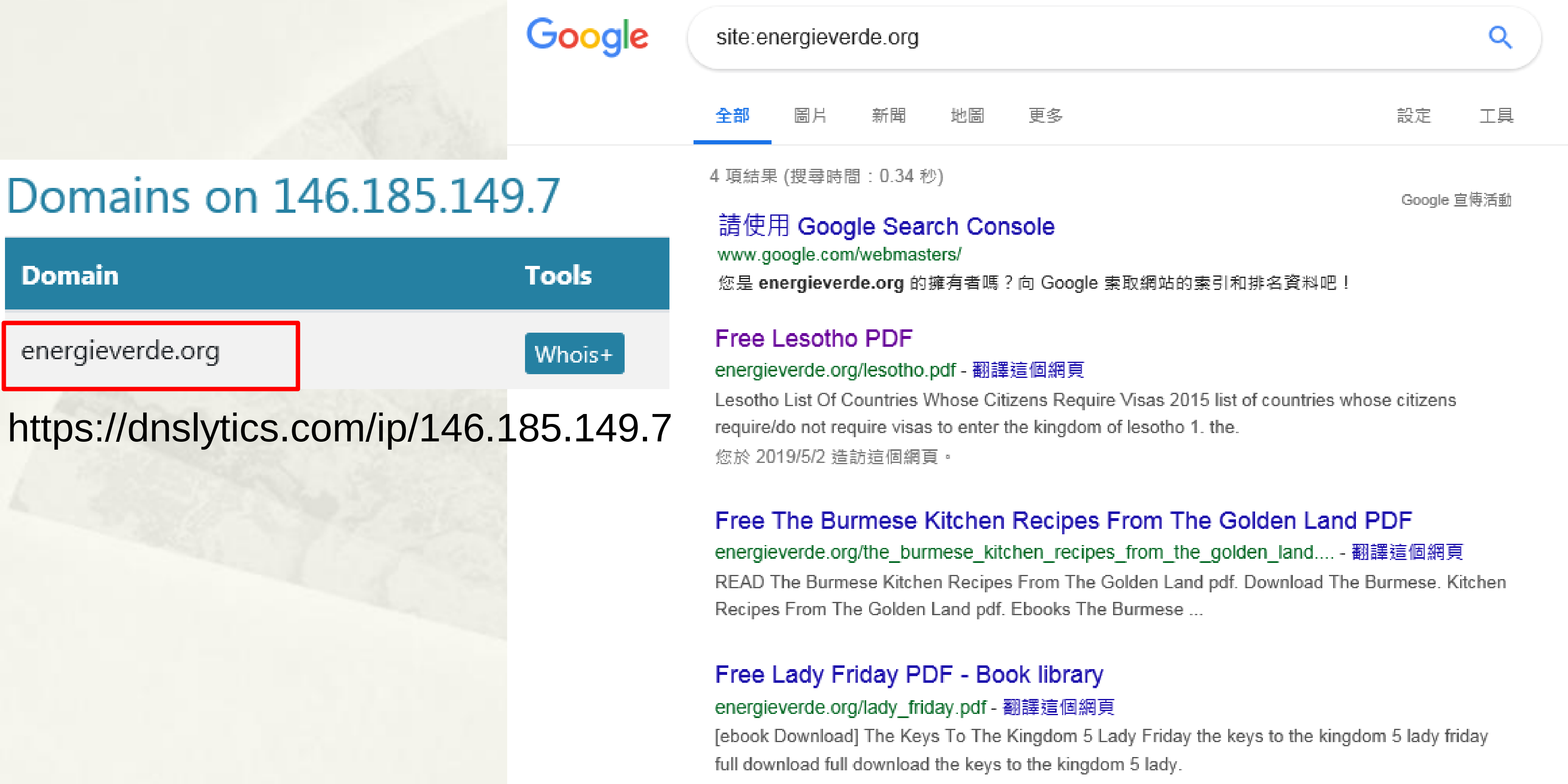
62.73.3.105/32

91.109.16.24/32



AS number	2588 (AS2588 / ASN2588)
Organization	SIA Latnet
Country	Latvia (LV)
Allocation date	1993-06-18 by RIPE
Number of IPv4 addresses	119,808
ASRank (based on number of IPs)	1,792
Number of IP prefixes	5 (IPv4) 1 (IPv6)
AS has bogon prefixes	No
Number of peers	4 (IPv4) 1 (IPv6)

Web site: energieverde.org True or Fake?



Domains on 146.185.149.7

Domain	Tools
energieverde.org	Whois+

https://dnslytics.com/ip/146.185.149.7

site:energieverde.org

4 項結果 (搜尋時間：0.34 秒)

Google 宣傳活動

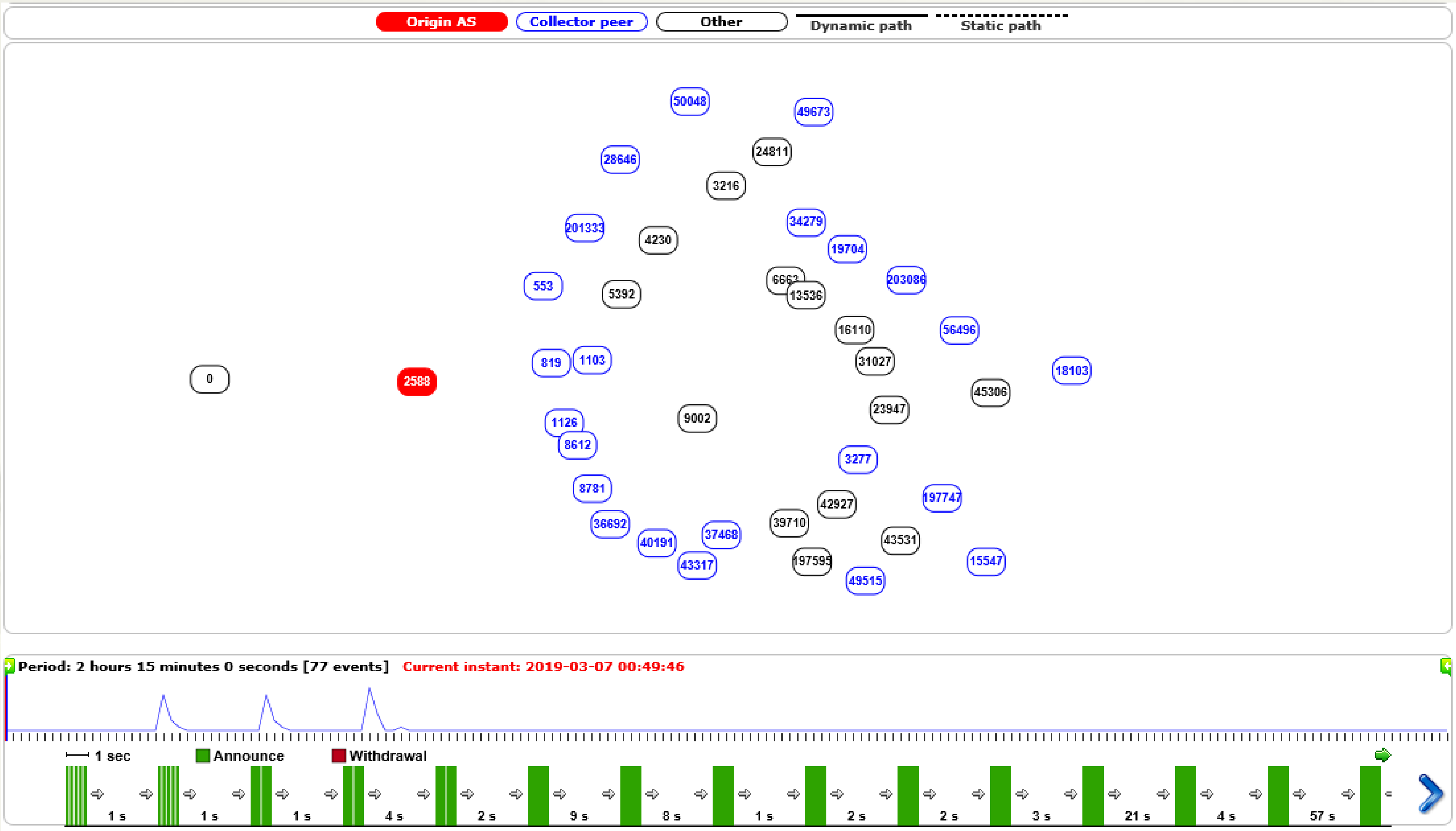
請使用 Google Search Console
www.google.com/webmasters/
您是 **energieverde.org** 的擁有者嗎？向 Google 索取網站的索引和排名資料吧！

Free Lesotho PDF
energieverde.org/lesotho.pdf - 翻譯這個網頁
Lesotho List Of Countries Whose Citizens Require Visas 2015 list of countries whose citizens require/do not require visas to enter the kingdom of lesotho 1. the.
您於 2019/5/2 造訪這個網頁。

Free The Burmese Kitchen Recipes From The Golden Land PDF
energieverde.org/the_burmese_kitchen_recipes_from_the_golden_land.... - 翻譯這個網頁
READ The Burmese Kitchen Recipes From The Golden Land pdf. Download The Burmese. Kitchen Recipes From The Golden Land pdf. Ebooks The Burmese ...

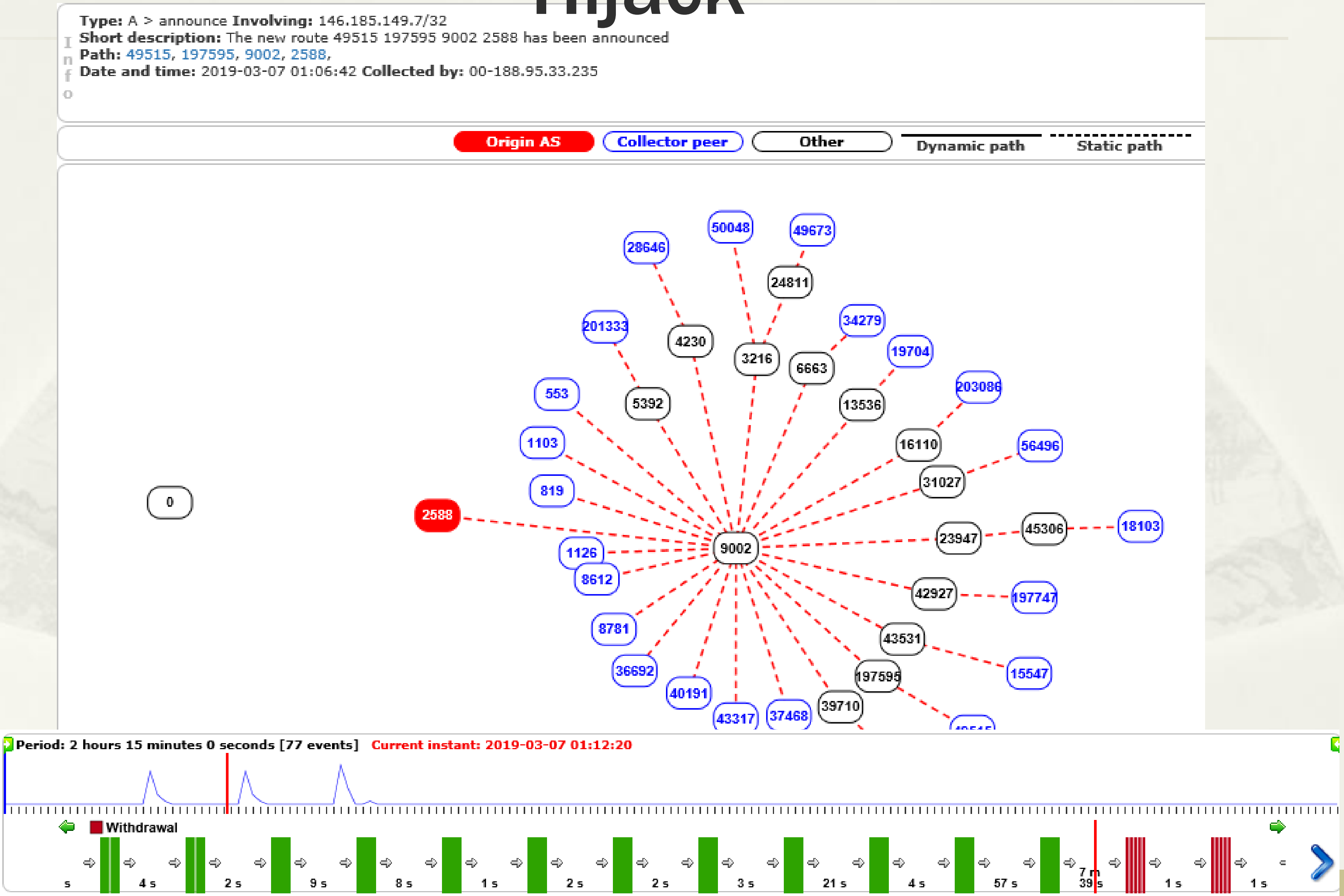
Free Lady Friday PDF - Book library
energieverde.org/lady_friday.pdf - 翻譯這個網頁
[ebook Download] The Keys To The Kingdom 5 Lady Friday the keys to the kingdom 5 lady friday full download full download the keys to the kingdom 5 lady.

146.185.149.7/32 Before Hijack



Period: 2 hours 15 minutes 0 seconds [77 events] Current instant: 2019-03-07 00:49:46

146.185.149.7/32 Hijack



Info

Type: A > announce **Involving:** 146.185.149.7/32
Short description: The new route 49515 197595 9002 2588 has been announced
Path: 49515, 197595, 9002, 2588,
Date and time: 2019-03-07 01:06:42 **Collected by:** 00-188.95.33.235

Period: 2 hours 15 minutes 0 seconds [77 events] Current instant: 2019-03-07 01:12:20

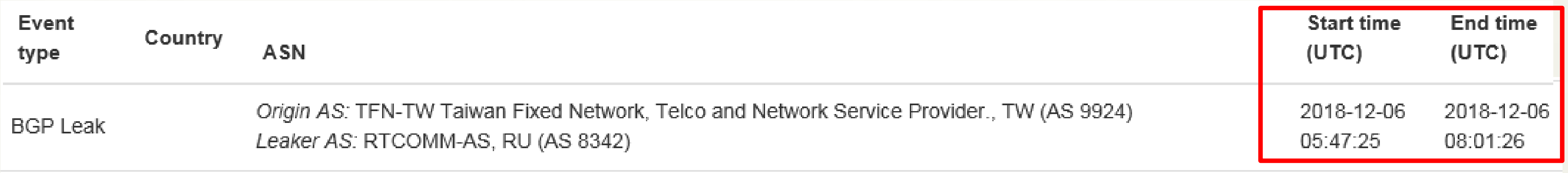
Prevention for Complete BGP Hijacks

- Accept only Prefixes with Length /24 and Less

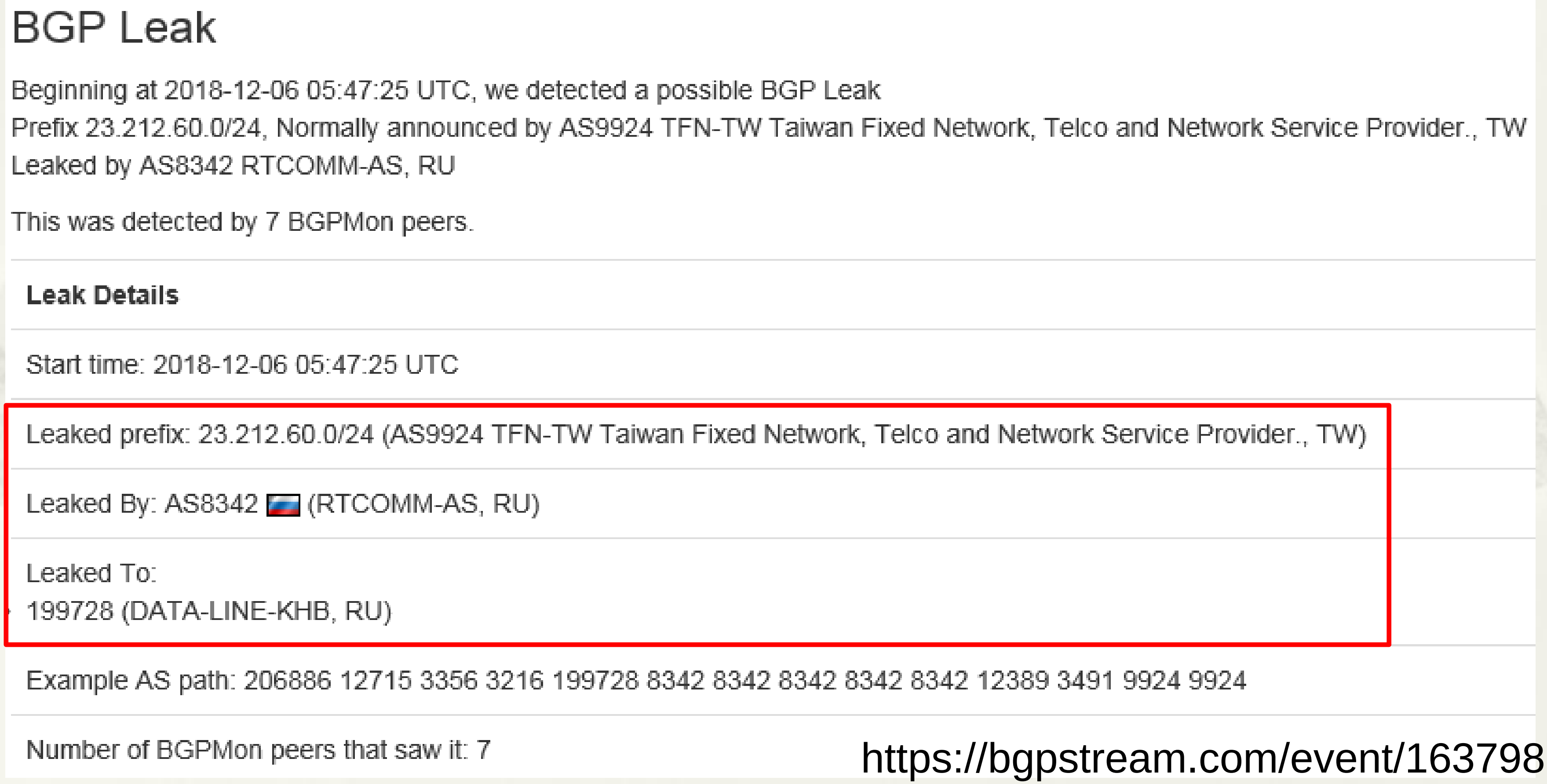
```
ip prefix-list filter_in
  seq 10 permit 0.0.0.0/0 le 24
router bgp 1659
  neighbor 200.1.1.1 prefix-list filter_in in
```

BGP Leaks

BGP Leaks 23.212.60.0/24



Event type	Country	ASN	Start time (UTC)	End time (UTC)
BGP Leak		*Origin AS:* TFN-TW Taiwan Fixed Network, Telco and Network Service Provider., TW (AS 9924) *Leaker AS:* RTCOMM-AS, RU (AS 8342)	2018-12-06 05:47:25	2018-12-06 08:01:26



BGP Leak

Beginning at 2018-12-06 05:47:25 UTC, we detected a possible BGP Leak
Prefix 23.212.60.0/24, Normally announced by AS9924 TFN-TW Taiwan Fixed Network, Telco and Network Service Provider., TW
Leaked by AS8342 RTCOMM-AS, RU

This was detected by 7 BGPMon peers.

Leak Details

Start time: 2018-12-06 05:47:25 UTC

Leaked prefix: 23.212.60.0/24 (AS9924 TFN-TW Taiwan Fixed Network, Telco and Network Service Provider., TW)

Leaked By: AS8342 🇷🇺 (RTCOMM-AS, RU)

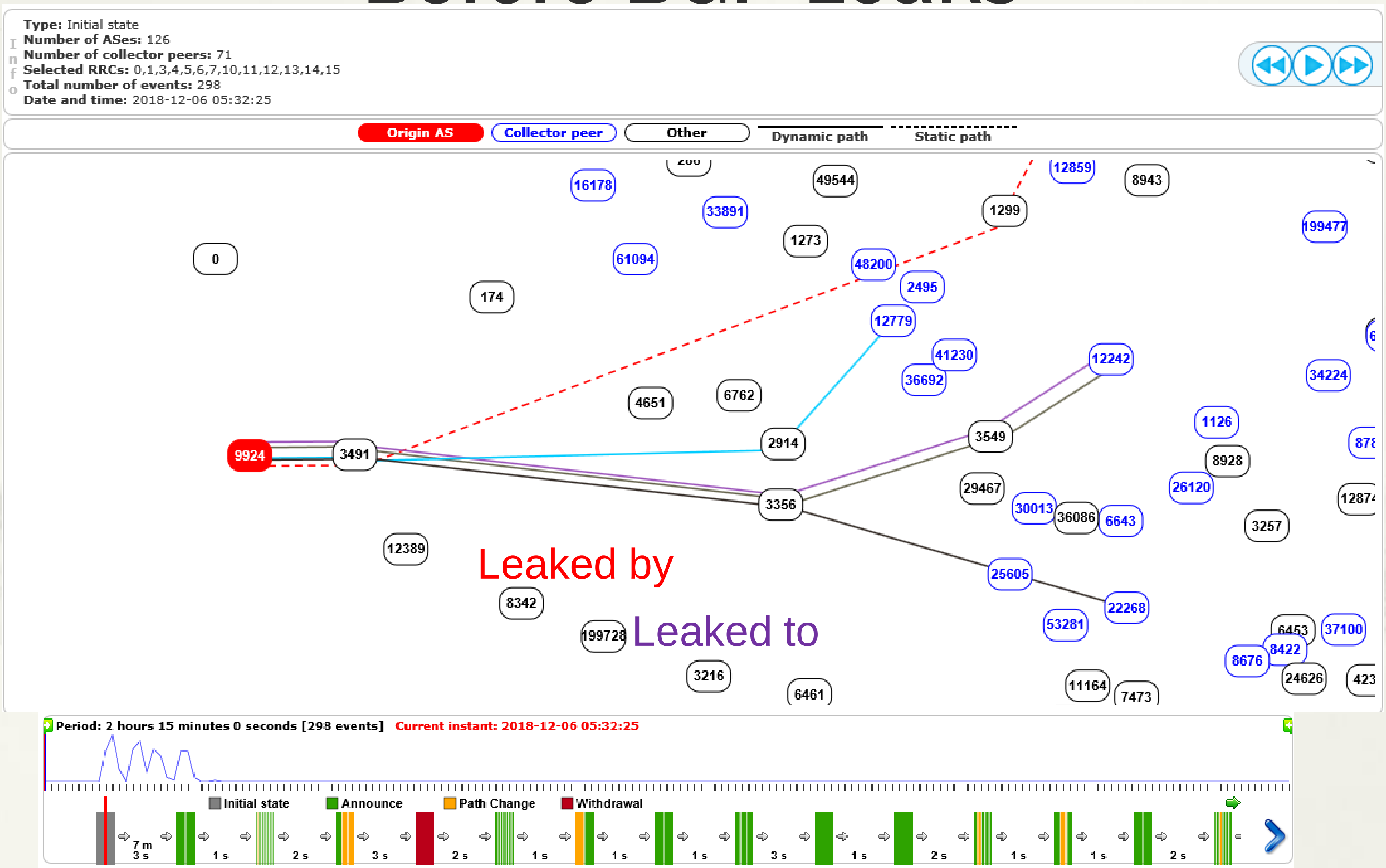
Leaked To:
199728 (DATA-LINE-KHB, RU)

Example AS path: 206886 12715 3356 3216 199728 8342 8342 8342 8342 8342 12389 3491 9924 9924

Number of BGPMon peers that saw it: 7

https://bgpstream.com/event/163798

23.212.60.0/24
Before BGP Leaks



Type: Initial state
Number of ASes: 126
Number of collector peers: 71
Selected RRCs: 0,1,3,4,5,6,7,10,11,12,13,14,15
Total number of events: 298
Date and time: 2018-12-06 05:32:25

Origin AS | Collector peer | Other | Dynamic path | Static path

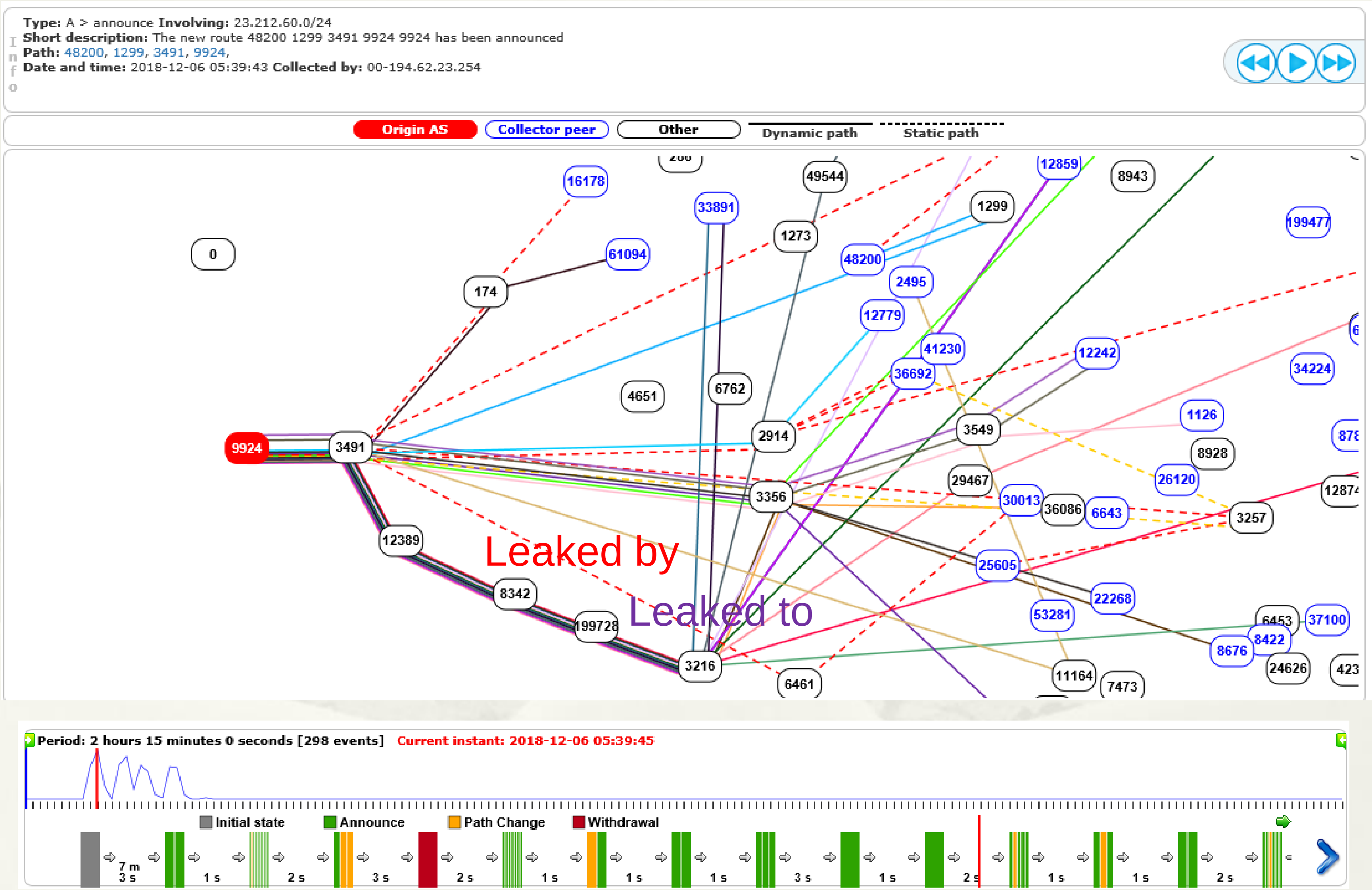
Period: 2 hours 15 minutes 0 seconds [298 events] **Current instant: 2018-12-06 05:32:25**

🟩 Initial state 🟩 Announce 🟧 Path Change 🟥 Withdrawal

Leaked by

Leaked to

23.212.60.0/24
BGP Leaks



Type: A > announce **Involving:** 23.212.60.0/24
Short description: The new route 48200 1299 3491 9924 9924 has been announced
Path: 48200, 1299, 3491, 9924,
Date and time: 2018-12-06 05:39:43 **Collected by:** 00-194.62.23.254

Period: 2 hours 15 minutes 0 seconds [298 events] Current instant: 2018-12-06 05:39:45

Leaked by

Leaked to

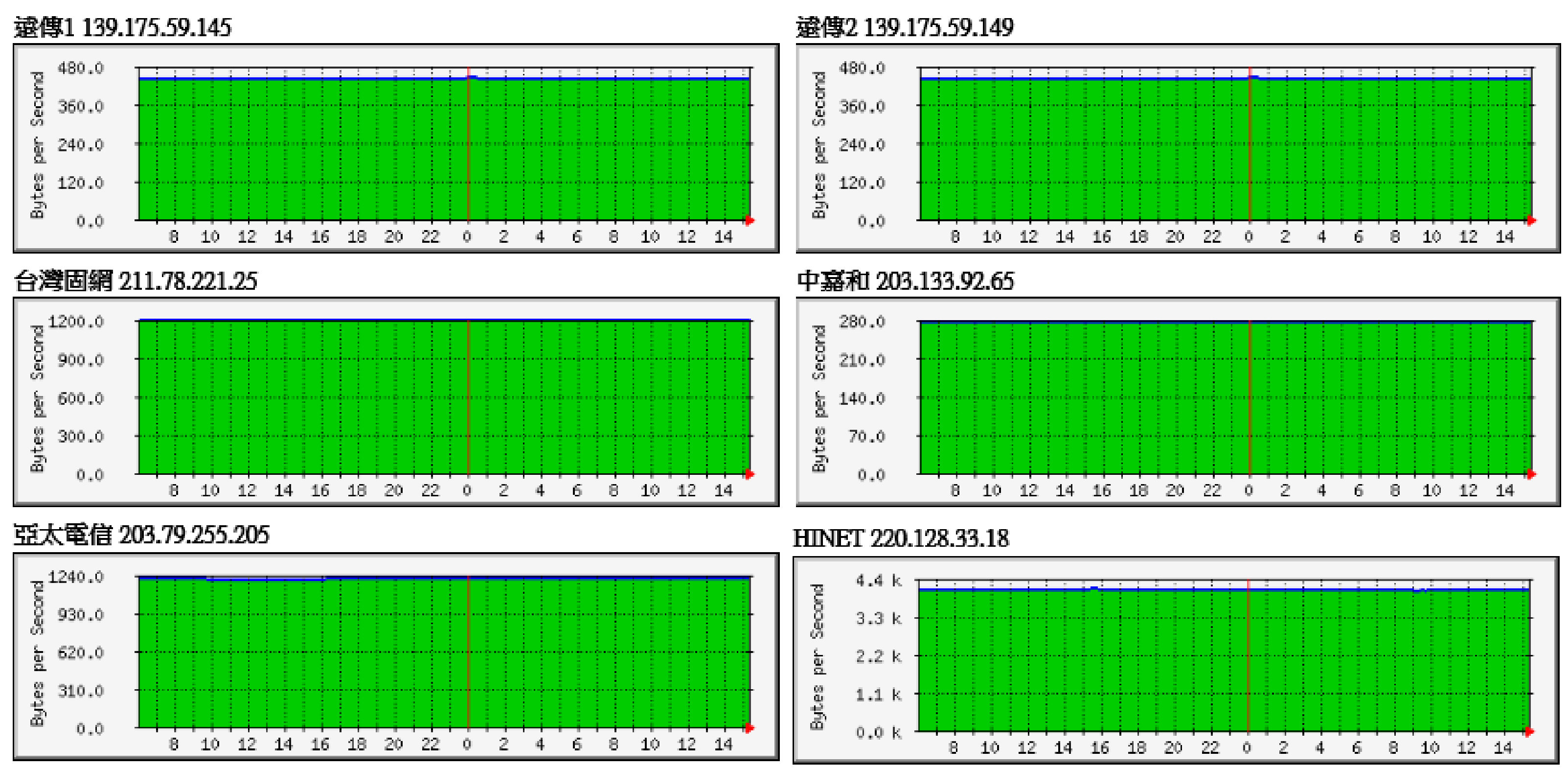
Prevention for BGP Hijacks & Leaks

- BGP Hijacks
  - One BGP Neighbor 宣告所有 Internet 網段都在它身上
- BGP Leaks
  - One BGP Neighbor 宣告所有 Internet 網段經過它為最佳路徑
- How to prevent?
  - Limit Maximum-Prefix

```
(config)# router bgp 1659
(config-router)# neighbor ip-address maximum-prefix 3000
```

臺大區網不同 ISP 收到之 BGP Prefix 筆數統計

- http://www.tp1rc.edu.tw/mrtg/bgp_prefix.html



遠傳1 139.175.59.145

遠傳2 139.175.59.149

台灣固網 211.78.221.25

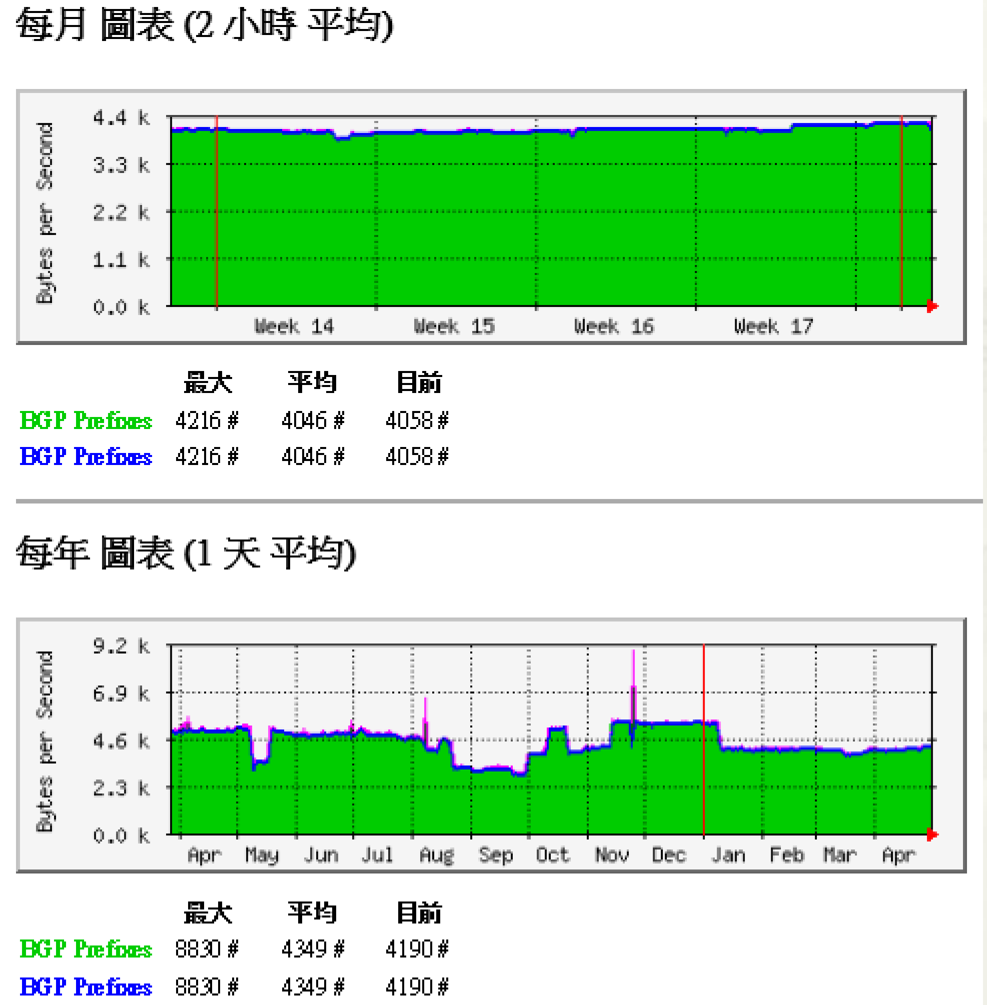
中嘉和 203.133.92.65

亞太電信 203.79.255.205

HINET 220.128.33.18

Hinet BGP prefix

- http://www.tp1rc.edu.tw/mrtg/bgp_220.128.33.18.html



每月 圖表 (2 小時 平均)

	最大	平均	目前
BGP Prefixes	4216 #	4046 #	4058 #
BGP Prefixes	4216 #	4046 #	4058 #

每年 圖表 (1 天 平均)

	最大	平均	目前
BGP Prefixes	8830 #	4349 #	4190 #
BGP Prefixes	8830 #	4349 #	4190 #

簡報完畢
謝謝