2015年に起きた BGP経路ハイジャック

吉村 知夏 Twitter:@chikayossy
NTT Communications / NTT America

JANOG37 in Nagoya

Monterey, CA

Who am I?

- 吉村 知夏 (Chika Yoshimura)
- NTT Communications所属
  - AS2914のネットワークエンジニア
  - 海外出向中
  - GIN (AS2914) で3年くらい
  - OCN (AS4713)で10年くらい
- 趣味
  - ドヤリング (＝Starbucksでmacを開いて仕事をしているフリをする)
  - 旅行
  - iPhoneで写真撮影 (資料内で使ってます)


November 06 2015…


05:52:05 UTC…
※AS2914はUTCで運用しています。
Somewhere in the US
4

大規模BGP Hijack発生！

A Huge BGP Hijack Issue Occurred

BGPMON Now part of OpenDNS

HOME BLOG ABOUT US PRODUCTS AND SERVICES NEWS AND PRESS CLIEN

Large scale BGP hijack out of India

Posted by Andree Toonk - November 6, 2015 - Hijack - 1 Comment

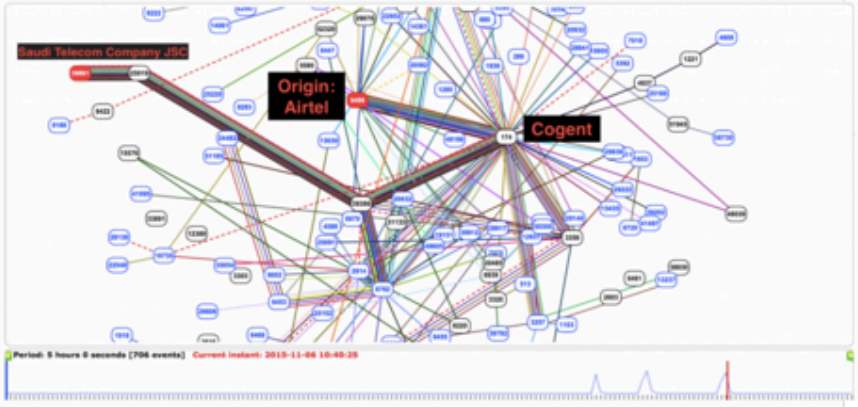
BGP hijacks happen every day, some of them affect more networks than others and every now and then there's a major incident that affects thousands of networks. Our monitoring systems keep an eye out for our users and if you would like to have a general idea of what's going on in the world of BGP incidents, keep an eye on BGPstream.com. Earlier today we detected one of those major incidents that affected thousands of networks.

Starting at 05:52 UTC, AS9498 (BHARTI Airtel Ltd.) started to claim ownership for thousands of prefixes by originating them in BGP. This affected prefixes for over two thousand unique organizations (Autonomous systems).

Our systems detected origin AS changes (hijacks) for 16,123 prefixes. The scope and impact was different per prefix but to give you an idea, about 7,600 of these announcements were seen by five or more of our peers (unique peers ASns) and 6,000 of these were seen by more than 10 of our peers.

One of the reasons this was so widespread is because large networks such as AS174 (Cogent Communications) and AS52320 (GlobeNet Cabos Submarinos VZLA) accepted and propagated these prefixes to their peers and customers.

The BGPlay visualization below shows an example hijack for a prefix normally announced by AS39891 Saudi Telecom Company JSC.



http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/

BGP Hijack とは

- 他ASのIPアドレス帯 を、非正規のASから勝手にBGP広告する(*) こと
  - (*) BGP Origin ASを偽って広告
- たとえば 2.16.65.0/24
  - AS2914のIPアドレス帯域です
  - AS2914以外が自分のものとしてBGP広告した場合 ≒ BGP経路hijack
- hijackされたBGP経路を、正規の経路と信じてしまうことがあります。
- 正規経路と信じた場合、hijack元のASへトラフィックが流れることがあります。
- けっこう発生してます。
  - 2015/08/01-2015/12/31：850回以上 (BGPStream調べ)

Typical Root Causes

- 意図的に、悪意を持ってやる (Maliciously)
- 非意図的に、悪意なくやる (Non-maliciously)
  - つまり、運用ミス
  - (例) 経路のリーク
    - 例えば、eBGPで受信した経路をIGPにre-distribute
    - そのIGP経路を、今度は別のeBGPにリークしちゃうとか
  - (例)検証用に使ってた経路を外にリーク
    - 検証環境でフルルートを使うことはたまにある
  - BGPフィルターのミスが多いと推測

- (FYI) Multiple origin
  - 2つ以上のOrigin ASから経路広報すること
  - 経路hijackではない

BGP Hijack Issue on Nov 6

- BGPMonによると:
  - 2015/11/06 05:52 – 14:40 UTC
  - AS9498 (Bharti Airtel) が、9498をOrigin ASとして複数のprefixをBGP広告
  - およそ2000AS、16123prefixがhijackされた
    - AS3257/GTT, AS4755/Tata Communications etc
    - AS2914/NTT Communications (Yes it's us!)
  - hijackは日常的に起きているが、比較的大きなhijackの一つだった。数千ネットワークが影響を受けた。
- http://www.bgpmon.net/large-scale-bgp-hijack-out-of-india/

Root Cause of the Hijack Issue

- 今のところ不明
  - AS2914からAS9498にヒアリング→Root Causeについては返答なし
  - BGPMonも情報なし
  - NANOG ML等でも情報なし
- 実際のhijack経路から推測するに…
  - eBGPからもらった -> IGP -> eBGP とリークしたのかな…?
  - BGPフィルター書き間違っちゃったのかな…?
- いろいろ推測はできるが、結局のところRoot Causeはよく分からない

Nov 6のAS2914の状況

AS2914 Sumo and Tanuki stickers

AS2914 Operational Timestamp

- Nov 06 同僚がhijackに気づく
- Nov 06 AS2914 NOC -> AS9498へメール
- Nov 07 AS2914 NOC -> AS9498へ再度メール
- Nov 07 AS9498から返信あり
  - 原因については言及なし
- Nov 07 AS2914 NOC -> AS9498へメール。原因について再度ヒアリング
- その後は返答なし

- BGPMonのメンバーと連携して影響範囲を調査


BGP Hijackの影響は
2つに分けられる
Two Different Impacts When a Hijack Issue Occurs

(A) Other ASes Prefixes Hijacked and Advertised to Our ASes

- hijack経路が自ASへ流入する
  - トラフィックへの影響は？: ある
    - 自AS -> hijack経路あてのトラフィックが、hijack元に流れる。
  - どこから流入？: 主にピアや上流ASから
    - 顧客ASからも流入する可能性はあるが、一般的には考えにくい
    - prefix-based filterを書いていることが多いため
  - 防御策はないの？: あるにはある
    - Origin Validation (以下便宜的にOV) を行えば:
      - hijack経路の流入を防ぐことができる
      - …が、OVを行うためには各prefixのROAが必要
      - ROAの作成は各ASに任されている
      - つまり、自ASだけで完結する防御策ではない
    - BGPフィルタを適切に書けば:
      - hijack経路の流入を防ぐことができる
      - 自ASでできる、ほぼ唯一の防御策
      - ただし、運用上、厳しいフィルタを書けないところもある

(B) Our Prefixes Hijacked and Advertised to the Internet

- 自ASの経路がhijackされ、世の中に流通する
  - トラフィックへの影響は？: ある
    - 他AS -> 自ASあてのトラフィックが、hijack元に流れる
  - どこへ流通？
    - 経路流入ポイントでBGPフィルタをしてなかったり、してもすり抜けてしまったAS
    - OVをしてないAS
  - 防御策は？: ほぼ無い
    - 世の中への経路流通を止めることは、基本的にできない
    - 経路の受け入れポリシーやフィルタ設定は、各ASに任されているため（各ASでとても厳しいフィルタを書いたり、OVを設定する必要がある）
    - ROAを発行しておけば:
      - OVを行っているASへの流通を止めることができる
      - …が、OVを他ASへ強制することはできない
      - つまり、自ASだけで完結する防御策ではない

AS2914ではどうだったの？

…then how about the situation in AS2914?

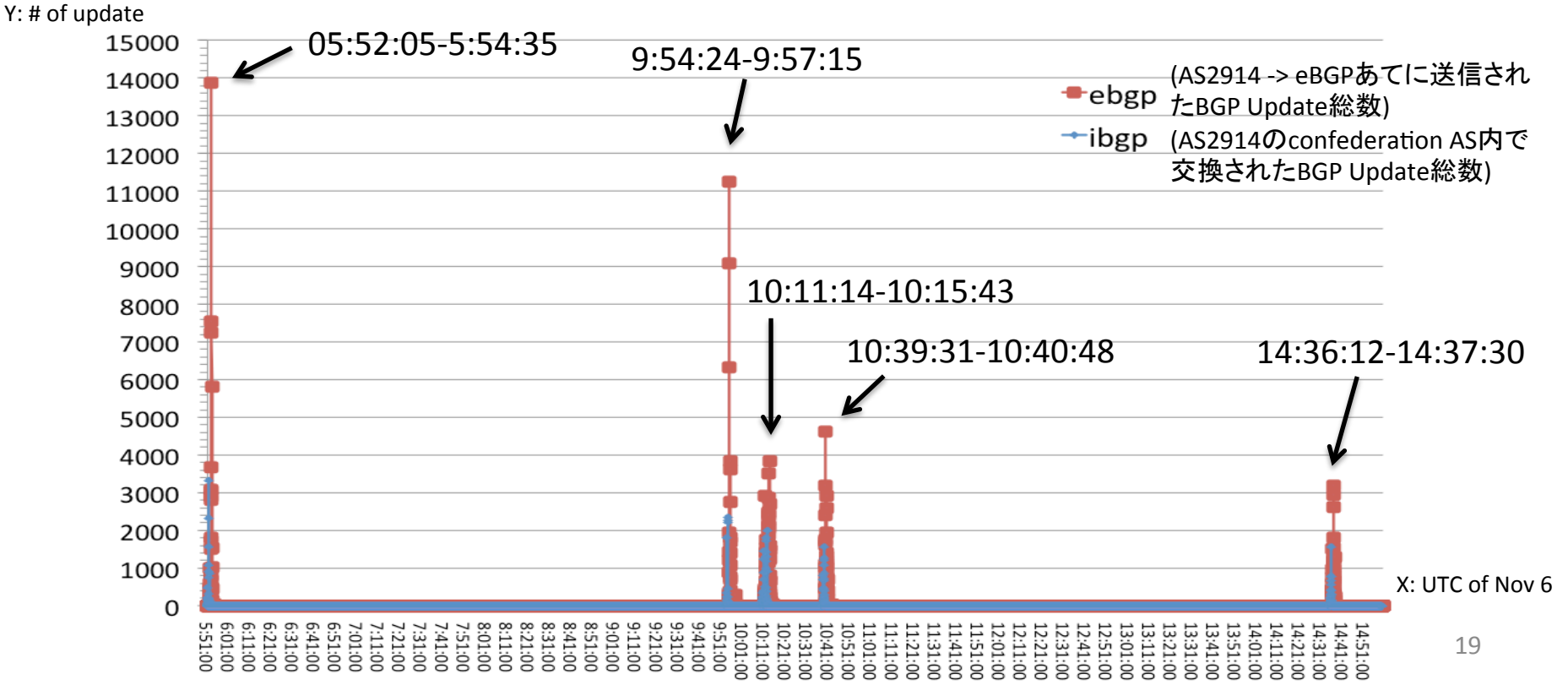

(A)Hijack経路、
流入した？
Did you receive any hijacked prefix?
科学忍者隊 IPENG
Fighting 2914

流入しました
Yes, we received some of them

- 2015/11/06 05:52:05 - 14:37:41 UTC
- 4513 prefixes (IPv4: 4512, IPv6: 1)
  - BGPMonの発表と差分があるのは、hijackの影響範囲はそもそもASによって異なるためです。ここからお見せするデータは、AS2914で観測したデータです。
  - 影響経路が少ない理由は？：当日言います
- 主にピアから流入しました
  - 上位ASはもともと存在しない
  - 顧客AS向けにはガチガチのfilterを書いている
  - ピアAS向けには、ざっくりとしたfilterを書いている
- 自ASの経路は流入しませんでした
  - 自ASの経路は、もともとAS2914内部に高LPで存在

BGP Update of Hijacked Prefixes

- hijack経路のBGP Update総数
  - ibgp: 70255 updates
  - eBGP: 286282 updates
- AS2914の全バックボーンルータは約200台。世界各国に約70 POP。



Hijacked prefix ranges received from other ASes

- 1.x、5.x、8.x などのアドレス帯域がhijackされている
- （再掲）AS2914の観測データです。実際には、ここに書かれていないPrefixもhijackされていたと推測しています。

range	# of hijacked prefix
1.x	1331
2.x	175
5.x	1771
6.x	34
8.x	858
12.x	229
14.x	8
23.x	1
24.x	2
27.x	96
61.x	1
64.x	1
125.x	1
177.x	4
2c0f:fe90::	1
total	4513

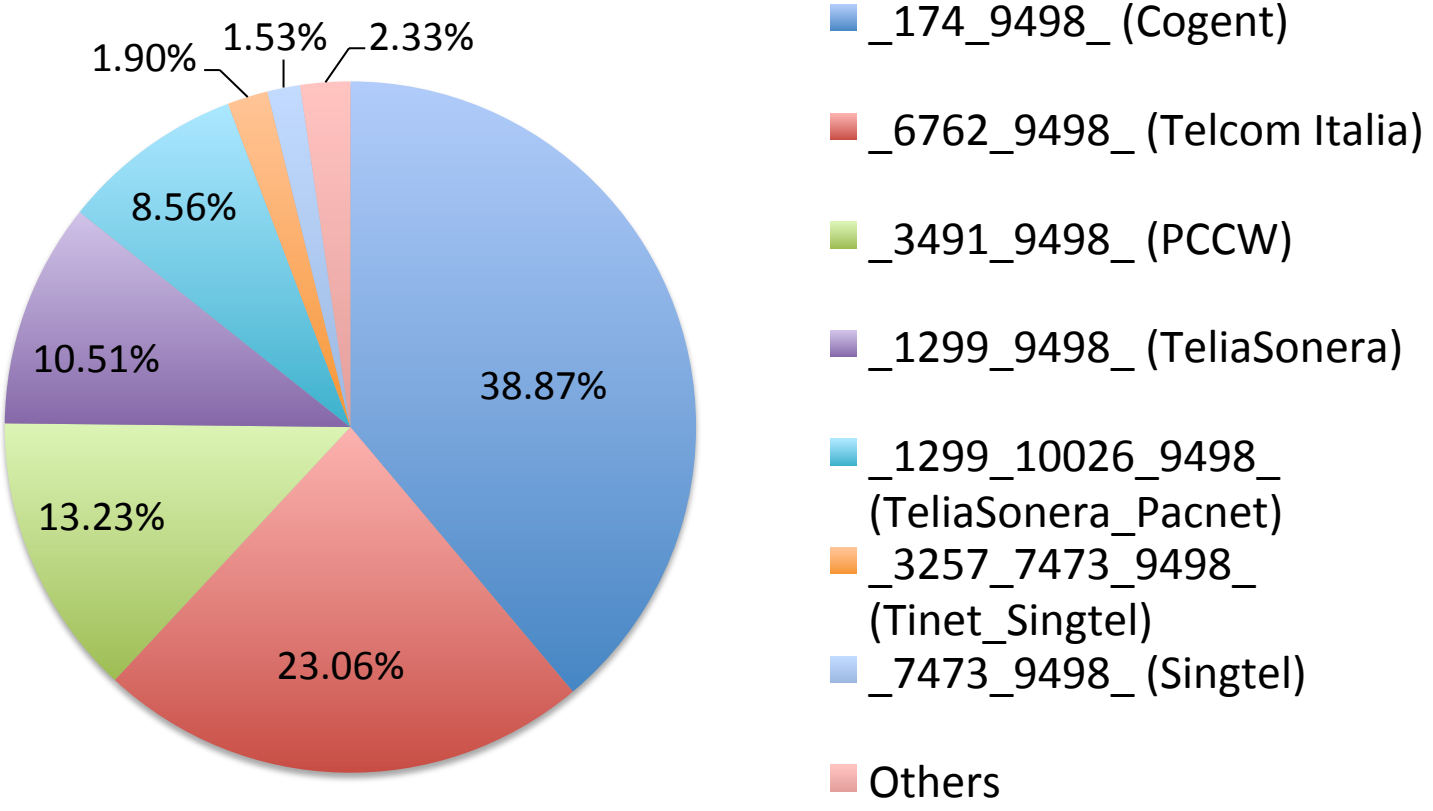
(a part of) Original ASes of Hijacked Prefixes

- hijack経路が本来属するAS
- AS2914の観測データから10件だけを抜粋したものです
- 実際にはもっと多くのASがあります

ASN	Name	Country
39891	Saudi Telecom Company	SA
24378	Total Access Communication	TH
12586	GHOSTnet	DE
18403	The Corporation for Financing & Promoting Technology	VN
35819	Etihad Etisalat Company	SA
4788	TM Net	MY
38266	Vodafone Essar	IN
23089	Hotwire Communications	US
45083	Beijing CheeryZone Scitech	CN
21299	2DAY Telecom	KZ

Where did the hijacked prefixes come from?

- hijack経路がどこから流入してきたか
- AS2914のピア (主にTier1 ISPs) から流入してきている



AS2914 BGP Import Filters

- Peer
  - Bogon etc
  - uRPF
  - Max prefix filter
  - (a kind of) AS path filter
  - 相手はTier1なので、ほぼフルルートを広告してくる。このため、きめ細かなフィルターを書くことは非現実的。
- Customer
  - Bogon etc
  - uRPF
  - Max prefix filter
  - Prefix filter (based on IRR)

BGP Origin Validation

- してません

(B) AS2914のCIDR、hijackされた？

Were AS2914 CIDRs hijacked and advertised to the Internet?

AS2914 Sumo and Tanuki stickers

Hijackされました

Yes, our prefixes were hijacked

- AS2914のCIDRのうち、およそ300prefixがhijackされ、インターネットへ流通
- AS2914のCIDRは、お客様へのサービス用途に払い出していない (一部例外あり。BGPの接続用アドレスなど)
- このため、実質的な影響はなかった。

(A part of) Hijacked Prefixes – BGPMon調べ

announced_prefix	base_as	src_AS	start_time	Peer_count
2.16.65.0/24	2914	9498	2015-11-06 05:52:14	68
2.16.110.0/23	2914	9498	2015-11-06 05:52:20	49
2.17.196.0/22	2914	9498	2015-11-06 05:52:15	47
5.158.208.0/21	2914	9498	2015-11-06 05:52:19	37
2.21.16.0/20	2914	9498	2015-11-06 05:52:15	33
23.55.208.0/20	2914	9498	2015-11-06 05:52:26	10
23.67.64.0/22	2914	9498	2015-11-06 05:52:26	10
23.55.80.0/20	2914	9498	2015-11-06 05:52:26	10
23.38.110.0/23	2914	9498	2015-11-06 05:52:26	10
23.11.192.0/22	2914	9498	2015-11-06 05:52:23	10
23.4.32.0/20	2914	9498	2015-11-06 05:52:20	10
23.11.196.0/22	2914	9498	2015-11-06 05:52:23	10
23.200.240.0/20	2914	9498	2015-11-06 05:52:27	8
23.201.96.0/23	2914	9498	2015-11-06 05:52:27	8

影響がない？

- 自ASのPrefixがhijackされた時、実質的な影響有無は、「そのprefixを使ってどのようなサービスをしてるか」に依存する
- IP Whole Sale (Transitサービスを売ること)では、自ASのprefixは基本的に使わない
  - お客様ご自身のASでprefixをお持ちのため
- Consumer Services: 自ASのprefixをお客様に払い出し、使っていただく
- 同じTier1でも…
  - AT&Tなど: IP Whole Sale + Consumer Services
  - GIN: IP Whole Sale Only

Conclusion

- 11/6に大規模なHijackが起こりました
- Hijack元にコンタクトしましたRoot Causeは分かりませんでした
- AS2914へのサービスインパクトは、ほぼありませんでした
- サービスインパクトは、Hijackされたprefixをどのように使っているかに大きく依存します
- Tier1をはじめ、あらゆるASがHijack経路をばら撒かないようにするのが理想的です
- が、RPKI（に限らず新技術）を導入するかどうかは、コストパフォーマンスの判断が入ることが多いです。優れた技術であっても、積極的な導入はしないという現実解になることもあり、判断基準はASによってそれぞれです。

Thanks! Then Okada-san's Talk