不審なBGP経路広報

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

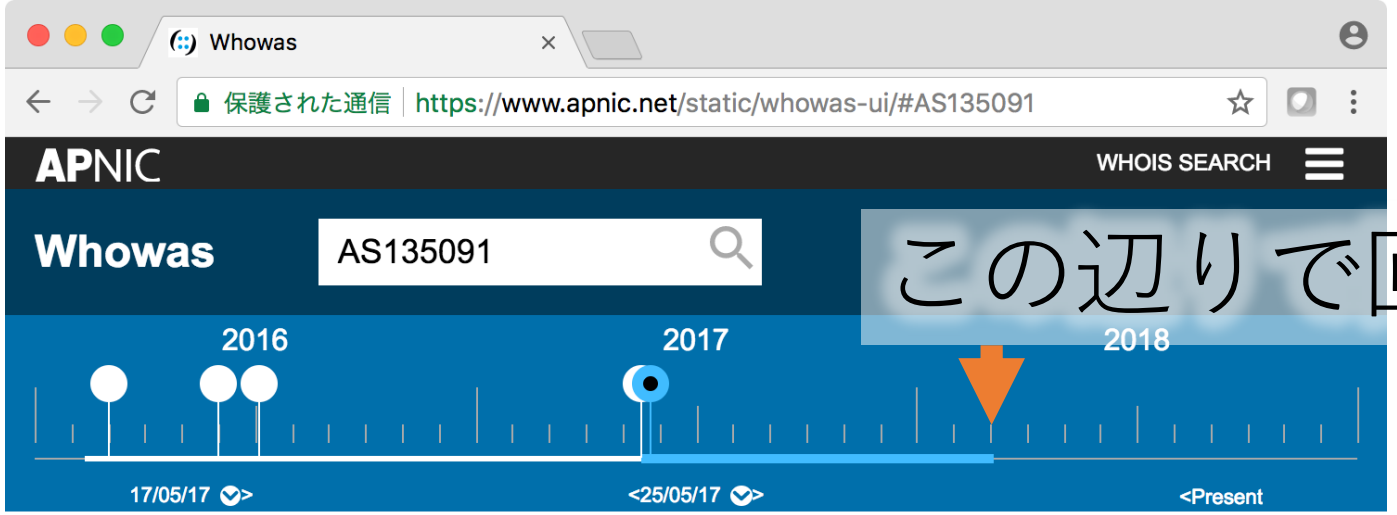
2015年
ISPにIPv4持込みして経路広報

- 経路ハイジャックされた話@JANOG36
  - https://www.janog.gr.jp/meeting/janog36/program/hijack
- IIJに移転したばかりのIPv4 prefixを、第三者に経路広告されていた
  - その依頼者はドメイン名や提出書類を偽装していた
  - 意図的な悪意ある行為だった模様
- 各所に連絡して広報の停止とかブロックリストからの解除とかを頑張った

2017年
未割り当てASから経路広報

- 某所から連絡
  - “An AS is hijacking a bunch of IPv4 prefixes, and even worse the AS is an APNIC *unassigned* AS”
- 経路生成に使われていたAS135091は未割り当て
  - APNICが回収済
- 様々な地域の大きな割り振りを勝手に広報
  - 27.146.0.0/16　MY
  - 42.128.0.0/16　CN
  - 130.21.0.0/16　US
  - 150.25.0.0/16　JP

  などなど



この辺りで回収

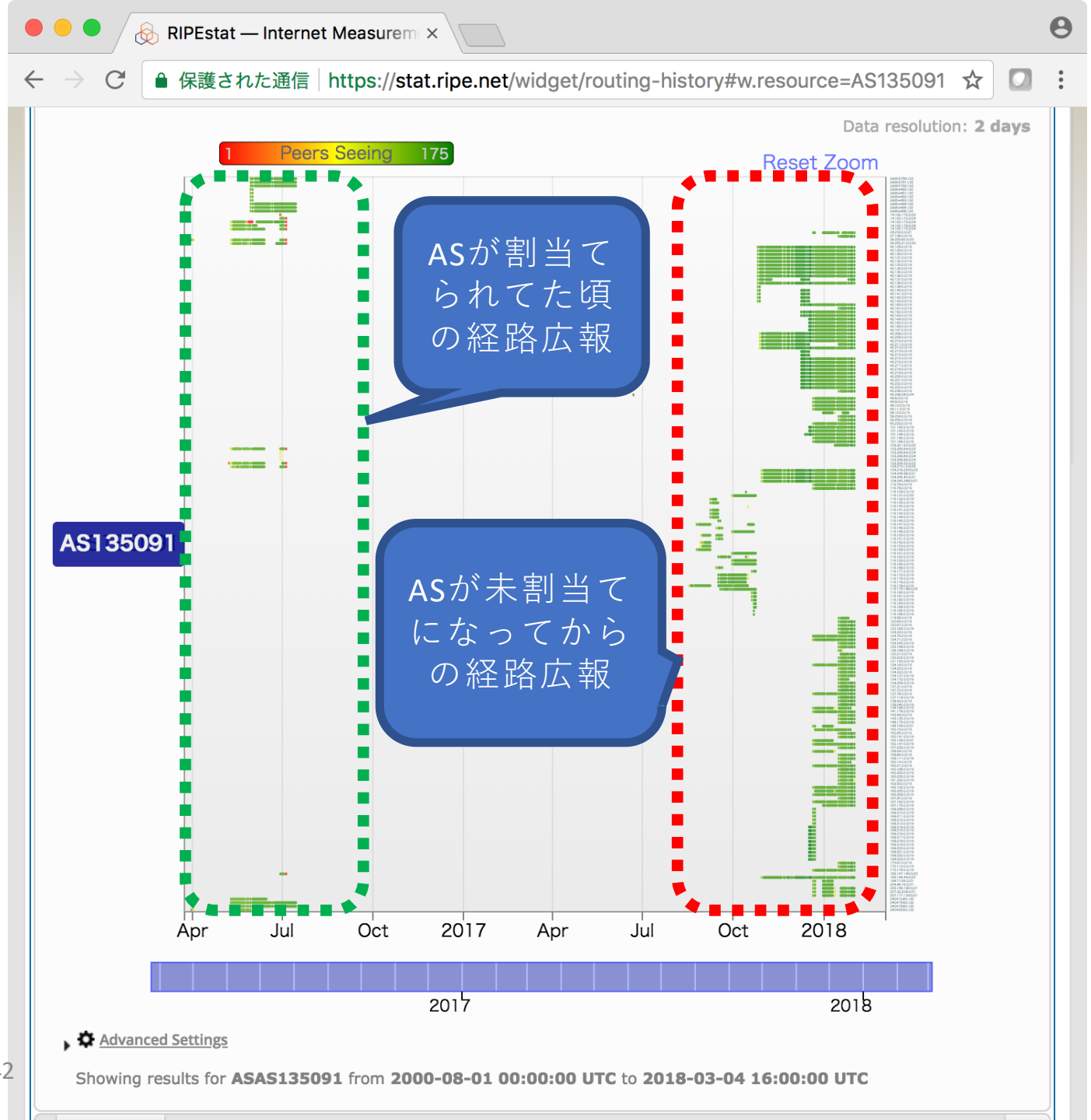
handle
AS135091
AS name
NODERUN-AS-AP
! country
~~PK~~
US
! description
~~NODE (PVT.) LIMITED~~
NODERUN INTERNET

---

handle
IRT-NODERUN-PK
name
IRT-NODERUN-PK
kind
group
address
Node (PVT.) Ltd, Near Saidu College of Sciences,, Saidu Sharif, Mingora, Mingora KPK 19200
email
Abuse@noderun.net
email
Abuse@noderun.net

---

handle
FA132-AP
name
Farid Ahmad
kind
individual
address
Node (PVT.) Ltd, Near Saidu College of Sciences,, Saidu Sharif, Mingora, Mingora KPK 19200
voice


RIPEstat — Internet Measurem
保護された通信 | https://stat.ripe.net/widget/routing-history#w.resource=AS135091
Data resolution: 2 days
1 Peers Seeing 175
Reset Zoom
ASが割当てられてた頃の経路広報
ASが未割当てになってからの経路広報
AS135091
Apr
Jul
Oct
2017
Apr
Jul
Oct
2018
2017
2018
Advanced Settings
Showing results for ASAS135091 from 2000-08-01 00:00:00 UTC to 2018-03-04 16:00:00 UTC

未割り当てASへの対応

- AS135091には連絡が取れない
  - AS番号は未割り当て
  - 広報しているprefixは全て他の組織のもの
- AS135091にトランジットを提供していた上流のASにひたすら連絡
  - 未割り当てなASをトランジットしてはいけない事
  - トランジット対象のprefixも全て疑わしい事
- 各方面から数日間に渡って連絡して広報停止

2018年
連絡の取れないASから経路広報

- JPNICの未割振りIPv4プールの一部をモニタ開始
  - 2018年6月1日にwhois登録及びJPIRRにroute objectを登録して、経路奉行にて観測開始
- 早速アラート検知
  - 2018年5月初旬ごろからAS136945が未割り振りブロックを次々と/24で広報していた模様
- AS136945に連絡するも一切反応なし
  - APNICにはAS136945と連絡取れない旨を報告済み
- 上流のBitcanal/AS197426に連絡したところ、ようやく広報停止


RIPEstat — Internet Measurem
保護された通信
https://stat.ripe.net/widget/routing-history#w.resource=AS136945
Data resolution: 12 days
1 Peers Seeing 174
Reset Zoom
AS136945
JPNICの
未割り振り
ブロック
2018
Feb
Mar
Apr
May
Jun
Advanced Settings
Report a bug
AS136945 from 2000-08-01 00:00:00 UTC to 2018-06-28 00:00:00 UTC

AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3

- NANOGに投稿されたポスト
  - AS3266が色々不審な経路を広報している
  - JPNIC管理分の歴史的PIがBitcanal/AS3266から広報されていたことを検知
- 念のため上流のBitcanal/AS197426に問い合わせ
  - その後広報停止したが、同時期にCogent/AS174がAS197426からの不審な経路広報を受信しない設定を導入した模様のため、誰の対応による停止か不明
- AS197426の信頼性は不明


RIPEstat — Internet Measurem
保護された通信 | https://stat.ripe.net/widget/routing-history#w.resource=AS3266
Data resolution: 12 days
1 Peers Seeing 175
Reset Zoom
AS3266
Apr Jul Oct 2017 Apr Jul Oct 2018 Apr
2017
2018
JPNICの
管理ブロック
Advanced Settings
Report a bug
AS3266 from 2000-08-01 00:00:00 UTC to 2018-06-28 00:00:00 UTC

手口の推察

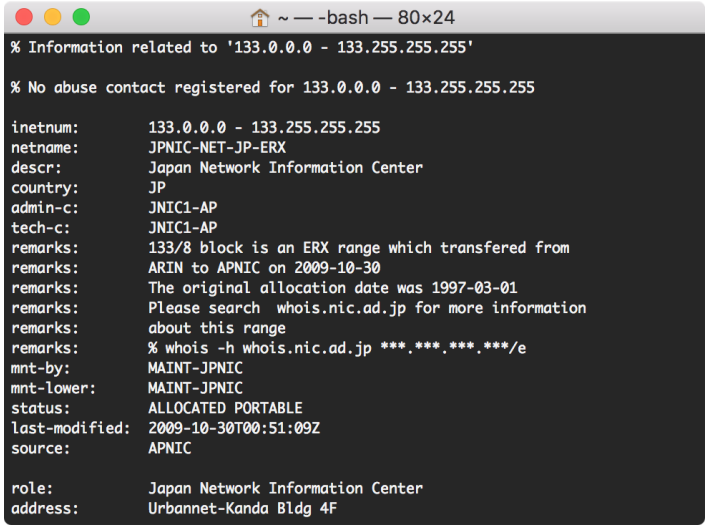
- 未利用な割り振り済み番号資源を勝手に利用
  - IPv4アドレス and AS番号
  - 何らかWhois情報がある＆経路広報されていない
- 連絡がつきにくい
  - Abuse主体を隠しやすい
- 勝手に売り買いしている可能性もある

その後のBitcanal/AS197426

- トランジットの停止
  - 6月末から7月上旬
  - 各上流ISPにて停止処理された模様
- IX接続の停止
  - 先週末
  - 各IX事業者にて接続解除処理された模様
- 7月11日、Bitcanal/AS197426及び、そこを経由する経路は全て見えなくなった状態
  - 数々の不審な経路広報を理由に、グローバルインターネットから切断された事例となりました

JPNIC未割り振りブロック

- RIR (APNIC) DB上はJPNICに割り振りされている
  - 例えば133.0.0.0/8



- 割り当て済みで、未利用と誤解されているかも

Pool Protection Project (PPP)

- IIJとJPNICの共同実験プロジェクト
  - JPNICが番号資源管理、IIJが実験環境の運用
- JPNICの管理するIPv4在庫を経路広報
  - 悪用を避けるために、“利用中”に見せかける
- トラヒックは基本的に吸い込むのみ
  - 将来的にはICMP unreachを返すかも
- 逆引きゾーンはSOA, NSのみ
  - PTRレコードは設定しない
- https://www.attn.jp/ppp/
  - にて詳細や統計情報を公開中

```
tech-c:      JP00163509
mnt-by:      MAINT-AS2522
source:      JPIRR
```

Nameservers for the reverse zones

```
ppp0.attn.jp
ppp1.attn.jp
```

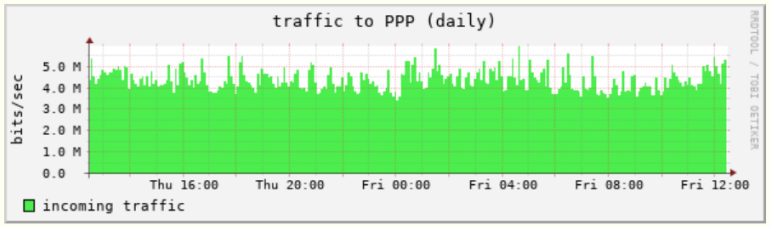
Contact

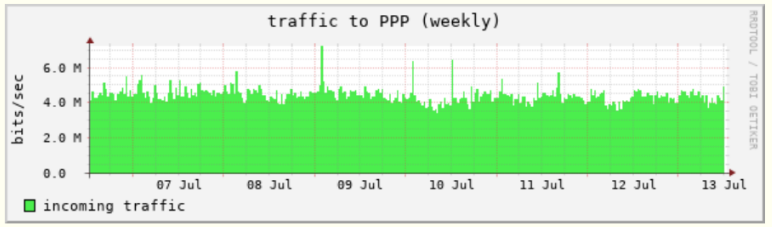
This is a joint project by IIJ and JPNIC.

To contact the project, please send emails to ppp-exp at nic.ad.jp

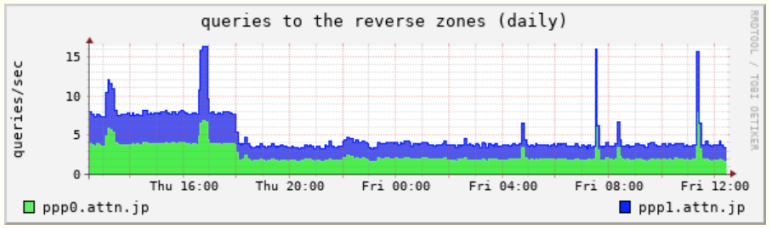
Statictics

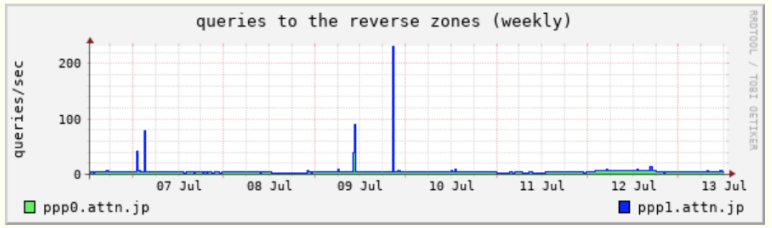
Traffic to PPP prefixes





DNS queries to reverse zones





Matsuzaki 'maz' Yoshinobu
maz@iij.ad.jp

不審な経路広告への対応

- しつこく連絡する
  - 広報元ASのNOC, Abuseやその他のコンタクト
  - その上流のISP
  - さらにその上流のISP
  - ASに連絡が取れない場合は管轄するRIRに通知
- 不正利用への萎縮効果を期待したい

取り＆逃げ事例

1. APNICに普通に/22を割り当て申請
   - Last /8ポリシーで1組織に1割り当ては行われる
2. ISPに持ち込みIPブロックの広報依頼
   - 申請書類はすごく真っ当なので受け入れられる
   - ISPが経路広報開始して、到達性を提供
3. 該当ブロックを何かの目的に使用
4. APNICの維持費用を払わない
   - 1年後の更新費用を払わない模様
5. 番号資源が回収される

取り＆逃げ事例でとばっちり

- ISPは未割り当て(回収済み)のIPv4を広報継続
  - 大抵の場合、APNICから広報停止依頼が来る
- ASとしての信頼度は下がってしまう
  - 知らない間に不審な経路広告に加担している状態

- 知見
  - 持ち込みIPブロックは、割り当て/割り振り状況を時々確認しましょう

PPPで気が付いたこと

- 逆引き問い合わせはprefix毎に頻度が違う

```
#prefix          total-query rate
61.122.16.0/22       55269 53.9736328125 query/ip
103.210.108.0/22     54317 53.0439453125 query/ip
133.112.0.0/16     3457855 52.7626800537109 query/ip
150.41.0.0/16      3054555 46.6088104248047 query/ip
158.200.0.0/16     2537312 38.71630859375 query/ip
192.47.97.0/24       13688 53.46875 query/ip
192.50.235.0/24      14286 55.8046875 query/ip
202.210.56.0/22      49709 48.5439453125 query/ip
203.178.8.0/24       12672 49.5 query/ip
203.179.64.0/20     189084 46.1630859375 query/ip
210.134.208.0/20    194448 47.47265625 query/ip
211.1.0.0/19        807504 98.572265625 query/ip
218.231.16.0/20     195105 47.633056640625 query/ip
219.101.112.0/20    210666 51.43212890625 query/ip
220.213.240.0/20    203221 49.614501953125 query/ip
```

普通に検索しても有用な情報がなかなか見つからない

地域指定で何か見えてきた

- 問い合わせ元に多かった地域を指定 (site:cn)

何故か設定例に載ってた！


```
iptables -I INPUT -s 211.1.0.0 -j DROP
iptables -I INPUT -s 211.1.0.0/16 -j DROP
```

同様の内容が、中国の様々なサイトに転載されている模様