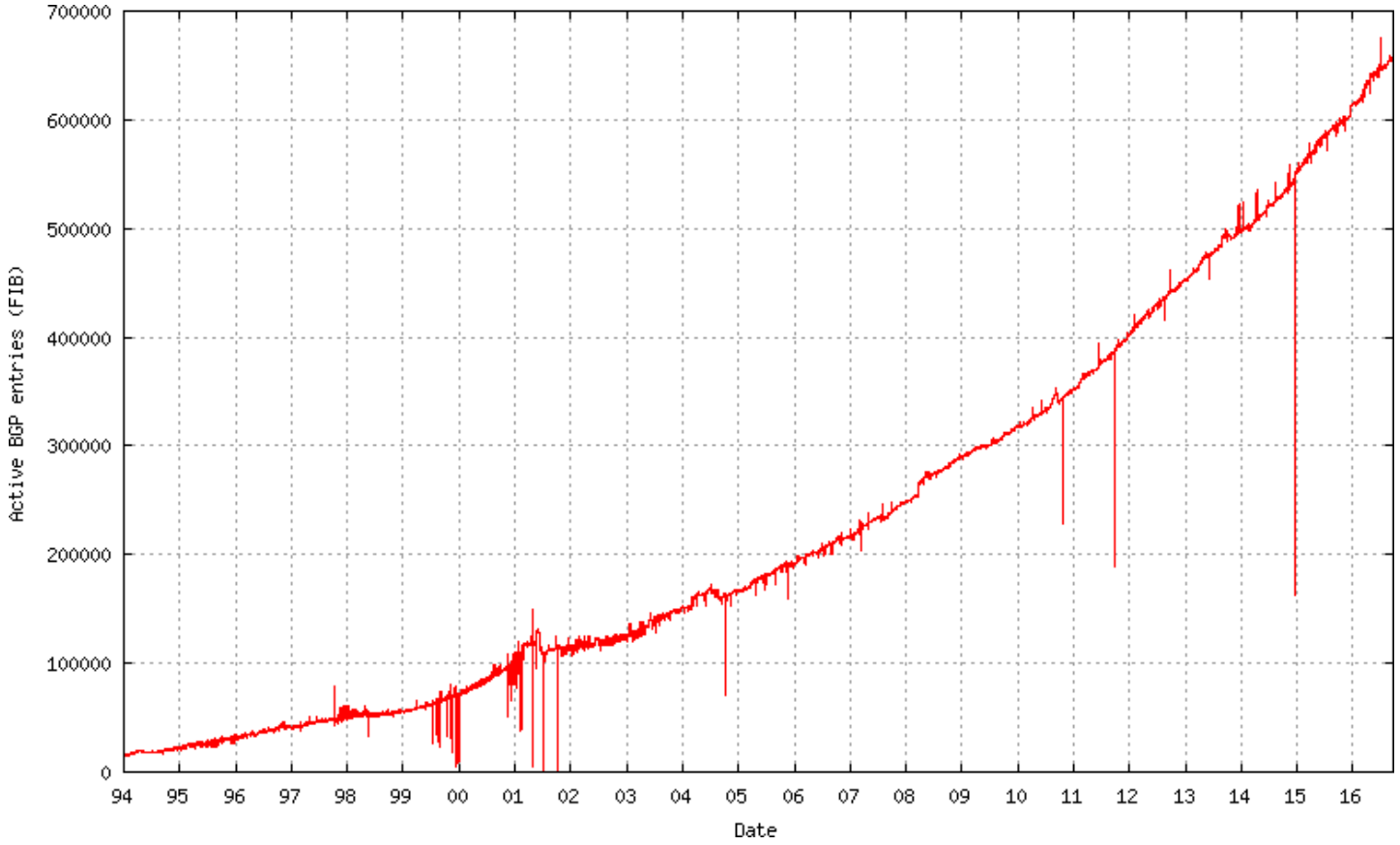
最近の経路と制御

Matsuzaki ‘maz’ Yoshinobu

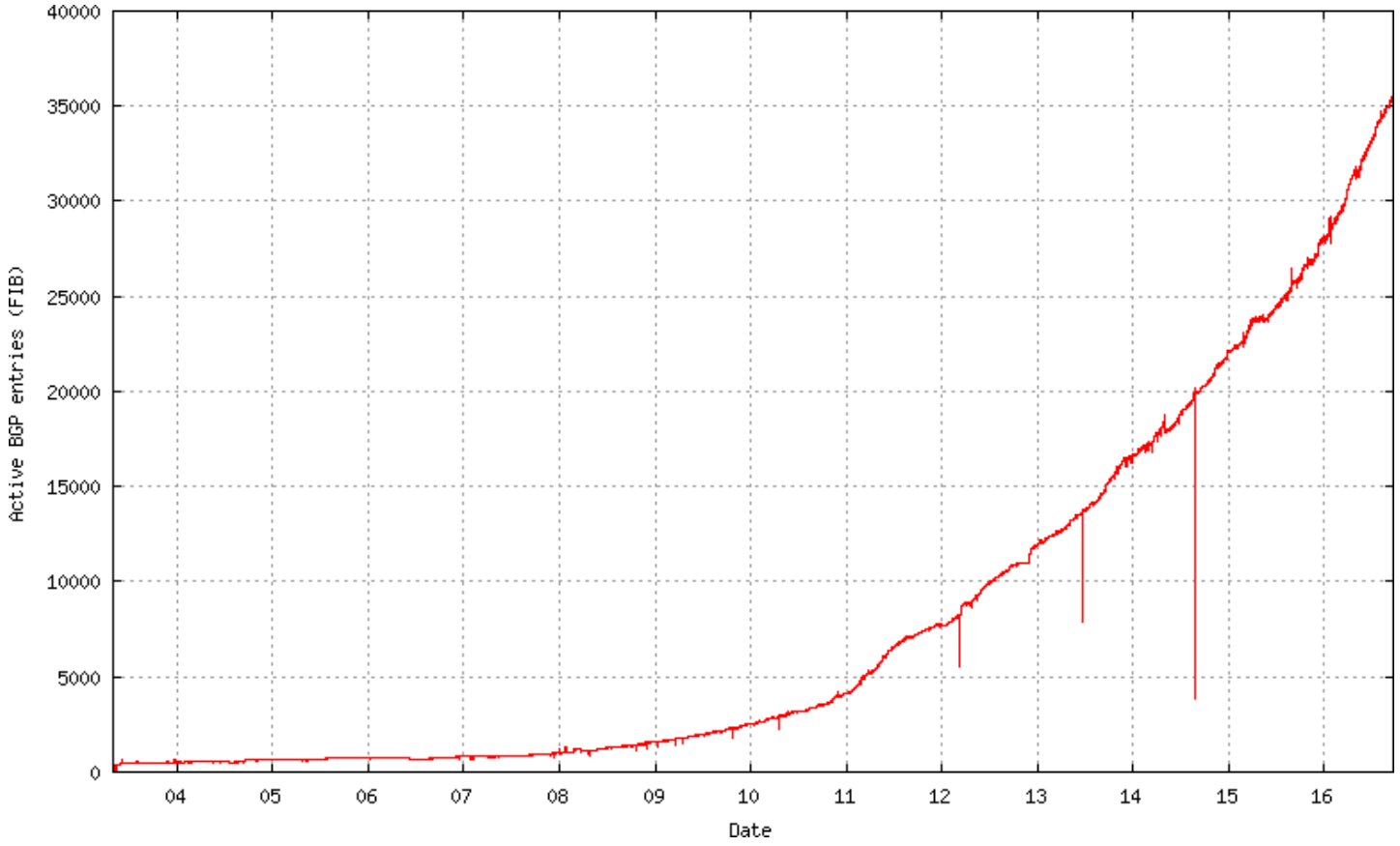
<maz@iij.ad.jp>

IPv4 full table



http://bgp.potaroo.net/as6447/

IPv6 full table



http://bgp.potaroo.net/v6/as6447/

その昔の経路ハイジャック

- 管理の怪しそうなネットワークから流れてきてた
  - 経路フィルタの怪しいネットワーク？
  - 管理の甘いルータや機器を乗っ取る？

最近の経路ハイジャック

- お金を払って有名どころの客になる
- 一部誤魔化して偽経路を流通させる

IPアドレスをISPに持ち込む

- ISPを納得させられれば攻撃成功
  - 客が持ち込むIPアドレスが正当に見えれば良い
  - 後はISPが経路広報してくれるので手が汚れない

- IIJが移転を受けたスペースがやられた事例
  - 偽のLetter of Authorityが提出されてた
  - それを信じたISPが勝手に経路広報
  - http://www.janog.gr.jp/meeting/janog36/download_file/view/163/179

IPアドレスをISPに持ち込む

- 利点
  - 使われていないスペースを使えばバレにくい
  - 世界のどこのISPでも大丈夫
  - BGPとかあんまり知らなくても大丈夫
- 欠点
  - 経路流通を制御できない
  - 悪いことに使うと苦情が使ってるISPまできちゃうかも

狙ったASと相互接続

- 狙ったISPと相互接続できれば攻撃成功
  - 相互接続できるだけの設備と環境を整えれば良い
  - 相互接続だと、顧客ほど厳密な経路フィルタにならない

- RIPE72で事例共有された件
  - IXPの客になって、対象のISPと相互接続
  - 適当なprefixを広報してspam送り放題
  - https://ripe72.ripe.net/presentations/45-Invisible_Hijacking.pdf

狙ったASと相互接続

- 利点
  - 狙ったところと通信してなさそうなprefixだったらなんでも使える
  - abuseの苦情はprefixの維持者に連絡される
  - looking glass等でも見つかりにくい
- 欠点
  - BGPとか相互接続の基礎知識がめんどくさい
  - 狙ったASがいそうなIXPやDCと契約する必要がある

教訓

- 保持しているIP空間は広報すべし
  - whois, IRR, RPKI等の整備
  - ハイジャック検知も併用
- 相互接続するASの素性はきちんと把握を
  - 知らないISPと接続するとき確認できてる？
  - そのASは本当にそこにいますか？
  - IXPは接続しているISPが使うAS番号を強制できない