Introduzione alla sicurezza di BGP

Marco d'Itri
<md@seeweb.it>
@rfc1036

Seeweb s.r.l.

Festival ICT 2015 - 11 novembre 2015

festival ICT

11 NOVEMBRE 2015
FIERA MILANO CONGRESSI

Internet: reti indipendenti che si scambiano traffico

Internet è un insieme di **reti indipendenti interconnesse** tra di loro, quindi occorre stabilire meccanismi tecnici e accordi commerciali che permettano a tutti di raggiungere chiunque altro.

Come fa una rete a sapere come raggiungerne un'altra?

- Non esiste un coordinamento centralizzato.
- Possono esserci più percorsi, che potrebbero essere rotti in un certo momento: occorre un meccanismo dinamico.
- Mediante il protocollo BGP ciascun lato di una interconnessione comunica all'altro per quali destinazioni vuole accettare traffico.

seeweb

Internet: diversi tipi di interconnessioni

Sono possibili vari accordi economici:

- **Cliente**: mi paga perché gli permetta di raggiungere il resto di Internet.
- **Peering**: ci accordiamo per scambiarci direttamente il traffico dei rispettivi clienti.
- **Transito**: sono io il cliente, e pago qualcuno perché mi permetta di raggiungere il resto di Internet.

Le basi del routing interdomain

Route

Le informazioni che individuano una rete, per esempio `192.175.48.0/24`, e come raggiungerla.

Il protocollo di routing BGP

- Serve per scambiare informazioni di routing dentro un autonomous system (internal BGP) o tra AS diversi (external BGP).
- Per esempio tra due peer o tra fornitore di transito e cliente

Autonomous system

- *Una entità con una unica politica di routing verso l'esterno.*
- Identificato da un numero: per esempio Seeweb è l'AS12637.
- Annuncia ai propri vicini le route per cui vuole ricevere traffico.

Un esempio pratico

```
md@spock> show route table inet.0 protocol bgp 192.175.48.0/24 terse

inet.0: 552304 destinations, 1425122 routes↩
  (551557 active, 12 holddown, 1188 hidden)
+ = Active Route, - = Last Active, * = Both

A V Destination      Metric 1   Metric 2  Next hop         AS path
* ? 192.175.48.0/24       150      10000                   112 I
  unverified                               >85.94.206.221
  ?                        150      10000                   12041 112 I
  unverified                               >217.29.66.124
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   12779 112 I
  unverified                               >217.29.66.65
  ?                        150      10000                   6939 16668 112 I
  unverified                               >217.29.66.125
  ?                        110     100000                   2914 16876 112 E
  unverified                               >81.25.202.193
```

Sicurezza del routing

Si può inviare ai propri vicini qualsiasi route: sono loro a dovere decidere quali accettare.

Per filtrare le route ricevute si creano, più o meno automaticamente, degli elenchi di route e/o di AS con cui le confronta il router.

A volte è oggettivamente difficile filtrare i propri peer, ma occorre impegnarsi di più per migliorare la sicurezza del routing di Internet.

È ingiustificabile non filtrare i propri clienti.

seeweb

Come sapere quali route qualcuno può annunciare?

Per esempio, un cliente o peer può usare:

- Record `route` o `route6` negli Internet Routing Registry (IRR), ma sono affidabili solo da RIPE e AFNIC e comunque non sempre sono tenuti aggiornati.
- Letter of authorization (LOA): può essere falsificata, richiede operazioni manuali, in pratica è usabile solo per i propri clienti.
- Attestazione crittografica mediante RPKI (origine) e BGPSEC (percorso): complesso, poco diffuso, vulnerabile ad attacchi giudiziari, aumenta la centralizzazione.

seeweb

IRR: un record `route`

```
route:          212.25.160.0/19
descr:          Seeweb srl
origin:         AS12637
mnt-by:         SEEWEB-MNT
created:        2006-02-09T08:08:36Z
last-modified:  2006-02-09T08:08:36Z
source:         RIPE
```

Autorizza AS12637 ad annunciare la rete `212.25.160.0/19`.

Routing Resilience Manifesto

Come migliorare la sicurezza e resilienza del sistema di routing globale?

Mutually Agreed Norms for Routing Security (MANRS)

- Prima raccomandazione pubblicata nel settembre 2014.
- Best practices minime da implementare per migliorare affidabilità e sicurezza del routing globale.
- Dimostra un impegno a seguirle da parte dei leader dell'industria: sponsorizzato da ISOC, tra i fondatori ci sono NTT, Level3, Comcast, CERNET.
- Seeweb aderisce nel febbraio 2015, prima rete italiana.

seeweb

Obiettivi

Dimostra la capacità dell'industria di autoregolamentarsi e crea consapevolezza grazie alla partecipazione dei leader.

- Promuove raccomandazioni minimali, adottabili facilmente da tutti e non controverse.
- Non pretende di risolvere tutti i problemi del routing e ci si aspetta che una rete ben gestita adotti misure più rigorose.
- Ogni piccolo passo aiuta.

seeweb

Le azioni raccomandate

- Impedire la propagazione di informazioni di routing non corrette.
- Impedire il traffico con IP sorgente falsificato.
- Facilitare le comunicazioni e il coordinamento tra gli operatori.
- Facilitare la validazione su scala globale delle informazioni di routing.

Nessuna di queste regole è innovativa: Seeweb ha potuto aderire immediatamente senza dovere modificare in alcun modo le proprie configurazioni o procedure.

seeweb

Informazioni di routing non corrette

Validare le informazioni di routing ricevute dai propri clienti, per impedire l'utilizzo non autorizzato di reti di terzi (per errore o per frodi...).

Esempi:

- Filtrare i propri clienti con prefix-list (non basta filtrare l'as-path!).
- Verificare la legittimità di ciascun nuovo prefisso annunciato prima di accettarlo.

Non richiede di validare le route dei propri peer, ma rimane comunque un'ottima idea...

seeweb

Traffico con IP sorgente falsificato

Impedire ai propri clienti diretti di falsificare gli IP sorgente del traffico che generano, il cosiddetto IP spoofing.

È indispensabile che il traffico generato dai propri utenti sia filtrato da meccanismi che permettano di utilizzare solo gli IP a loro assegnati.

Esempi:

- BCP 38 (RFC 2827): maggio 2000!
- ACL antispoofing
- `ip verify unicast source reachable-via rx`

seeweb

Comunicazioni e il coordinamento

Pubblicizzare i propri contatti H24 per essere prontamente rintracciabili dagli altri operatori in caso di necessità.

Esempi:

- Un oggetto role nel database whois di RIPE.
- Il sito del MIX.
- PeeringDB.

seeweb

Validazione delle informazioni di routing

Rendere possibile agli altri operatori la validazione delle proprie informazioni di routing, pubblicando l'elenco delle proprie reti e di quelle dei propri clienti.

Esempi:

- Pubblicare oggetti `as-set` e `route`/`route6` per le proprie reti.
- Richiedere lo stesso ai propri clienti.

Questo permette ai propri peer di validare i propri annunci.

seeweb

Un esperimento di hijacking

Metodologia

- Prendere in prestito da un amico una rete che non sta usando.
- Ottenere da un dump BGP l'elenco delle reti ricevute dai propri peer negli internet exchange.
- Cercare tra le reti di ciascuno dei propri peer un IP che risponda a ping.
- Annunciare "abusivamente" la rete prestata.
- Vedere quali dei precedenti IP rispondono ancora a ping fatti da questa rete.

seeweb

Un esperimento di hijacking: risultati

Quanti peer accettano una route annunciata abusivamente?

IX	peer totali	vulnerabili
MIX	109	59
NAMEX	18	6
TOP-IX	18	13
AMS-IX	462	441
DE-CIX	328	72
LINX	324	239
France-IX	110	101

Non ci sono scuse

Seeweb annuncia meno di 50 route, tutte correttamente registrate nel database di RIPE: le nostre sessioni possono facilmente essere validate automaticamente.

Incidenti famosi: AS7007

Il primo grande route leak globale

Il 25 aprile 1997 AS7007, un piccolo ISP statunitense, riceve da un proprio cliente 23000 route di terzi e le riannuncia al proprio transito, Sprint.

Queste route sono propagate globalmente e per cinque ore il routing di Internet è gravemente compromesso, anche a causa di problemi dei router primitivi.

Se AS7007 o Sprint avessero filtrato il proprio cliente non sarebbe successo nulla di grave!

Incidenti famosi: il Pakistan rompe Youtube

Un maldestro tentativo di censura

Il 24 febbraio 2008 Pakistan Telecom, nel tentativo di adempiere a una richiesta governativa di censurare Youtube, annuncia abusivamente parte di una loro rete, che viene propagata dal loro transito PCCW.

Per due ore e quindici minuti Youtube non funziona per tutta o parte di Internet.

Se PCCW avesse filtrato il proprio cliente non sarebbe successo nulla!

seeweb

Incidenti famosi: Hacking Team, i Carabinieri e Azienda X

I Carabinieri suggeriscono ad Azienda X di annunciare abusivamente una rete di un provider russo, per potere comunicare con alcuni trojan forniti da Hacking Team di cui avevano perso il controllo per motivi tecnici.

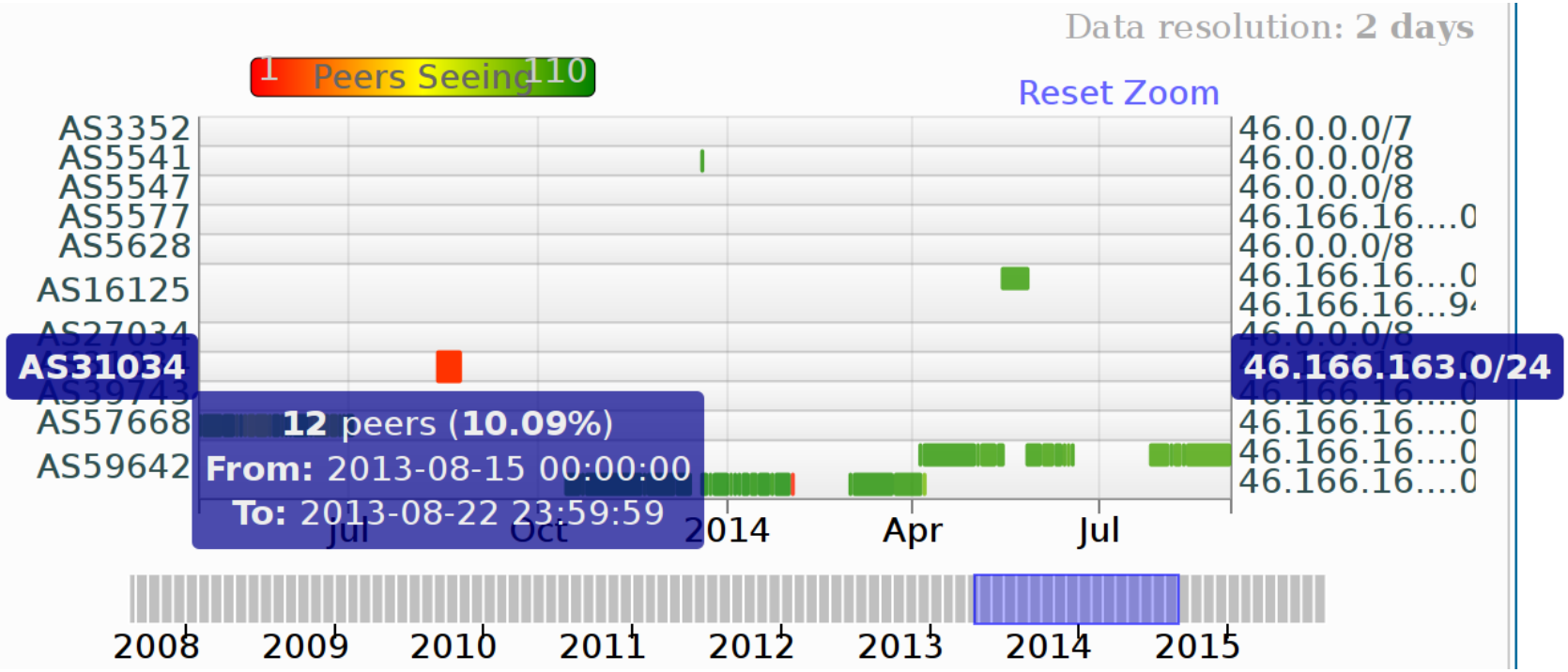
Azienda X per una settimana annuncia di proposito una rete di terzi senza il loro permesso, che viene propagata anche all'estero.

Se avessimo strumenti migliori nessuno dei peer di Azienda X avrebbe inconsapevolmente accettato questa route!

seeweb

Analisi di un hijacking

Grazie al servizio RIPEstat ho potuto verificare velocemente che la rete 46.166.163.0/24 era stata annunciata da Azienda X:



Poi l'ho confermato in modo dettagliato analizzando un dump delle tabelle BGP archiviato da RIPE.

Domande?

`http://www.linux.it/~md/text/bgp-security-fict2015.pdf`

(Google . . . Marco d'Itri . . . I feel lucky)

seeweb