Bogons: pacchetti IP non validi sulle WAN

In un precedente articolo[1] abbiamo già discusso del problema dei pacchetti IPv4 con indirizzo sorgente falso. Questi pacchetti sono tipicamente usati per possibili attacchi, i più semplici dei quali sono attacchi di tipo Denial-of-Service. IPv4 non è stato creato con meccanismi che permettano di identificare certamente chi è il mittente dei pacchetti e la soluzione migliore al momento a questo problema è di utilizzare tecniche crittografiche per identificare i propri corrispondenti. Il problema è notevole e si manifesta *indirettamente* anche in effetti che ormai vediamo tutti i giorni, quali lo spam nella posta elettronica.

In questo articolo saremo un po' meno pratici del solito poiché cercheremo di dare un'idea di come transitano i pacchetti nella rete informatica generalmente chiamata *internet* e come sia possibile rubare indirizzi IP od immettere pacchetti con indirizzi sorgenti falsi.

BGP

Possiamo inquadrare il problema a partire dalla nostra connessione ad internet. Qualcuno deve sapere quale strada devono fare i pacchetti che escono dalla nostra rete locale per giungere alla destinazione indicata. Queste informazioni sono contenute nelle così chiamate *Tavole di Routing*, ovvero di indirizzamento. Queste tavole sono presenti su tutte le macchine connesse ad una rete IP, ma hanno un ruolo più importante nei Router che devono indirizzare il traffico verso la destinazione finale. Le tavole sui router, a seconda del tipo di router e del suo ruolo, possono andare dalle più semplici con in pratica due righe, ad esempio una riga corrispondente alla propria rete interna e l'altra che indirizza a tutto internet, alle tavole presenti sui router di Internet Provider e Carrier che all'inizio del 2004 avevano circa 140.000 *Prefissi*.[2]

Come vengono popolate le tavole di routing di Internet Provider e Carrier? Il protocollo adottato è il Border Gateway Protocol (BGP) versione 4. BGP si basa su alcuni concetti semplici. Ad ogni organizzazione che deve implementare BGP viene assegnato un numero detto numero di Sistema Autonomo (AS). L'organizzazione stabilisce quindi almeno **due** connessioni BGP con altri Sistemi Autonomi, altri Internet Provider ad esempio. Una organizzazione può permettere il transito del traffico attraverso la propria rete interna verso altri Sistemi Autonomi oppure no, nel primo caso si dice un *AS di transito* ed è il caso tipico degli Internet Provider.

Consideriamo per primo il caso di una AS *non* di transito: in questo caso questa AS annuncia ai suoi corrispondenti BGP solo i propri prefissi, ovvero le classi di indirizzi IP pubblici presenti

1 ICT Security 21, Marzo 2004

2 I Prefissi sono gruppi di indirizzi IP organizzati in una classe, un prefisso è ad esempio 12.34.0.0/16 ovvero tutti gli indirizzi da 12.34.0.0 a 12.34.255.255; ad ogni prefisso è associata una *route* verso quella destinazione.

nella propria organizzazione e raggiungibili da internet. In cambio riceve dai propri corrispondenti le liste dei prefissi raggiungibili attraverso ognuno dei corrispondenti.

Il caso invece in cui una AS sia di transito, questa annuncia ad ogni corrispondente sia i propri prefissi che quelli che ha ricevuto da tutti gli altri corrispondenti: ad esempio avendo le AS 1, 2 e 3, la AS 1 annuncia a 2 i propri prefissi insieme a quelli ricevuti da 3, ed annuncia a 3 i propri prefissi insieme a quelli ricevuti da 2. In questo modo 2 avrà nelle proprie tavole di routing l'indicazione che per raggiungere la rete di 3 può passare attraverso 1.

Anche se visto così il protocollo potrebbe sembrare semplice, l'implementazione di BGP non è molto facile; non è questa però la sede per una discussione dei problemi di stabilità e di scelta dei percorsi migliori. Ci limiteremo qui a considerare alcuni semplici problemi relativi alla sicurezza.

I problemi

Bisogna ricordare che le tavole di routing contengono solo i percorsi di destinazione, in altre parole nessun controllo è fatto sugli indirizzi sorgenti presenti nei pacchetti. Il filtro sugli indirizzi sorgenti deve essere fatto al momento della partenza del pacchetto, ovvero quando esso lascia la propria AS di appartenenza. Una volta che un pacchetto è in transito non è più possibile verificare se l'indirizzo sorgente è stato forgiato,[3] è possibile unicamente controllare se l'indirizzo sorgente è tra quelli validi oppure tra quelli privati o non utilizzabili, come descritto nel precedente articolo.

Non esiste ancora un protocollo che permetta di verificare che tutti i pacchetti che lasciano la propria AS di origine abbiano un indirizzo IP valido, anche perché questo è sicuramente un problema di non facile soluzione. Al giorno d'oggi è lasciato alla buona volontà e *good netiquette* di chi gestisce le reti controllare che tutti i pacchetti originati nella propria AS ed in uscita dalla propria AS abbiano un indirizzo sorgente valido.

Per quanto riguarda invece le tavole di routing, bisogna dire che la maggior parte delle volte i problemi sorgono non da intenti malevoli ma da semplici errori di configurazione. Anche errori di configurazione possono però portare notevoli problemi. In particolare i più comuni problemi sono i seguenti:

- vengono inseriti numeri di AS inesistenti oppure privati
- vengono annunciati prefissi di indirizzi privati o riservati
- vengono annunciati prefissi di indirizzi altrui.

Consideriamo brevemente le conseguenze di questi tre problemi. Nel primo caso viene inserita nella lista di AS da attraversare un numero di un AS che non esiste, ovvero che non è assegnato a

3 Nel pacchetto non viene riportato il percorso effettuato e quindi non è possibile sapere con certezza quale sia l'origine del pacchetto stesso.

nessuno, oppure un numero privato o riservato.[4] E' ovvio che diventa per lo meno difficile che pacchetti possano giungere a destinazione se nel loro cammino devono attraversare AS che non esistono. Ricordiamoci che nell'esempio fatto precedentemente la AS 2 sapeva di poter raggiungere gli indirizzi IP della AS 3 passando attraverso la AS 1. Se invece della AS 1 ci fosse il numero di una AS inesistente, la AS 2 non sarebbe in grado di instradare i pacchetti verso la AS 3. Nella maggior parte dei casi i numeri di AS non validi sono utilizzati come AS iniziali e non di transito, e spesso per errore sono annunciati al mondo, ma vi sono casi in cui anche i numeri non validi sono di AS di transito. In media, su circa 17000 numeri di AS validi presenti nelle tavole BGP, ce ne sono circa 40 non validi.

Il secondo caso sembrerebbe il meno preoccupante, in quanto se una AS annuncia degli indirizzi privati, non dovrebbe ricevere alcun traffico. Però se la nostra organizzazione utilizza internamente degli indirizzi privati e i filtri od il NAT non sono configurati perfettamente, vi è la possibilità che il traffico interno finisca in internet e termini presso chi sta annunciando gli indirizzi privati. Ci si può però difendere facilmente da questo problema filtrando gli annunci dei prefissi che si ricevono dalle AS e bloccando il traffico verso gli indirizzi privati o riservati sui router di frontiera, un esempio è riportato in Tabella 1. Questo è anche possibile con un servizio BGP offerto da [3].

Il terzo caso è chiaramente quello che sembra più pericoloso, se gli indirizzi IP di una organizzazione sono annunciati anche da una altra, una delle due può *rubare* il traffico alla altra. In altre parole, annunciando gli stessi indirizzi IP di una altra azienda è possibile fare in modo che tutto il traffico, dalle visite ai siti web alla posta elettronica, raggiunga un altro. Non vi è una soluzione semplice a questo problema. In realtà vi è un controllo da parte di chi gestisce le reti a livello internazionale, e di solito un internet provider o carrier pone dei filtri in modo che gli annunci provenienti da AS non di transito siano solo i prefissi, ovvero degli indirizzi IP, ufficialmente assegnati a quelle AS. In ogni caso, conviene a internet provider e carrier effettuare dei controlli ed imporre delle limitazioni in quanto questi possono ridurre il traffico che passa sulle loro reti, il che è ovviamente nel loro interesse. Malgrado tutto ciò, vi sono in media più di 900 prefissi annunciati da più di un AS, nella maggior parte dei casi più per errore di configurazione che per altro.

Andrea Pasquinucci
Libero Professionista in Sicurezza Informatica
pasquinucci@ucci.it

4 Come per i numeri IP, esistono numeri di AS privati, da usarsi ad esempio solo all'interno di una azienda, riservati o non assegnati.

Riferimenti Bibliografici

[1] IANA http://www.iana.org/assignments/as-numbers

[2] BGP: RFC-1771 1772 1773 1774

[3] The Team Cymru Bogon Reference Page, http://www.cymru.com/Bogons/index.html

```
! our network is 1.2.0.0/16 and our AS is 99
ip prefix-list INGRESS seq 1  deny 0.0.0.0/0
ip prefix-list INGRESS seq 5  deny 0.0.0.0/8 le 32
ip prefix-list INGRESS seq 10 deny 10.0.0.0/8 le 32
ip prefix-list INGRESS seq 15 deny 127.0.0.0/8 le 32
ip prefix-list INGRESS seq 20 deny 172.16.0.0/12 le 32
ip prefix-list INGRESS seq 25 deny 169.254.0.0/16 le 32
ip prefix-list INGRESS seq 30 deny 192.0.2.0/24 le 32
ip prefix-list INGRESS seq 35 deny 192.168.0.0/16 le 32
ip prefix-list INGRESS seq 40 deny 198.18.0.0/15 le 32
ip prefix-list INGRESS seq 45 deny 224.0.0.0/3 le 32
ip prefix-list INGRESS seq 100 deny 1.2.0.0/16 le 32
ip prefix-list INGRESS seq 200 permit 0.0.0.0/0 ge 6 le 27
ip prefix-list INGRESS seq 300 deny 0.0.0.0/0 le 32

router bgp 99
 [...]
 neighbor 5.6.7.8 prefix-list INGRESS in
```

Tabella 1. Esempio di filtri sui prefissi BGP in entrata su router Cisco