

MANRS, perché?

Qual è il problema
che desideriamo risolvere?

WHAT ARE YOU WORKING ON?

TRYING TO FIX THE PROBLEMS I
CREATED WHEN I TRIED TO FIX
THE PROBLEMS I CREATED WHEN
I TRIED TO FIX THE PROBLEMS
I CREATED WHEN...



Il problema

Routing security

Solo nel 2017, 14mila eventi nell'ambito della sicurezza dell'instradamento su Internet hanno causato molteplici problemi, tra i quali sottrazione di dati, perdita di ricavi, danno all'immagine e oltre. Il 40% circa di tutti gli incidenti è causato da attacchi con una durata media di 19 ore per evento.

Routing security

L'ultimo enorme incidente è avvenuto lo scorso 12 novembre 2018 quando l'ISP nigeriano MAINONE ha accidentalmente oscurato Google a seguito di un errore di configurazione.

Routing security

Se non si vede Google amen.

*Ma se non si vedesse la
finale di
Champions?*





La questione d'onore e i problemi di routing

Il Border Gateway Protocol (BGP) si basa esclusivamente sulla fiducia tra gli ISP

- Creato prima che la sicurezza diventasse una preoccupazione
- Suppone che tutte le reti siano fidate
- Nessuna intrinseca validazione della legittimità degli aggiornamenti
- La catena della fiducia abbraccia tutti i continenti
- Mancanza di dati affidabili sulle risorse

Quali sono le minacce?

| Evento | Spiegazione | Ripercussioni | Soluzione |
|---|--|--|-------------------------------------|
| Dirottamento del prefisso o dell'instradamento | Un operatore di rete o un utente malintenzionato impersona un altro operatore di rete, fingendo che un server o una rete sia suo cliente. | I pacchetti vengono inoltrati nel posto sbagliato e possono causare attacchi di tipo DoS o intercettazione del traffico. | Politiche di filtro più efficaci |
| Perdite di instradamento | Un operatore di rete con più upstream (spesso a causa di errata configurazione) annuncia a un upstream che ha un instradamento verso una destinazione attraverso l'altro upstream. | Può essere utilizzato per l'ispezione del traffico e il riconoscimento. | Politiche di filtro più efficaci |
| Spoofing dell'indirizzo IP | Qualcuno crea pacchetti IP con un'origine falsa per nascondere l'identità del mittente o per impersonare un altro sistema informatico. | La causa principale degli attacchi DDoS | Validazione dell'indirizzo sorgente |

Collaborazione e Consenso

La tua sicurezza è nelle mani di qualcun altro.

Le azioni degli altri influenzano direttamente te e la tua sicurezza di rete (e viceversa).

Abbiamo bisogno di aspettative di sicurezza riconosciute a livello mondiale affinché tutti gli operatori di rete aumentino il livello di sicurezza dell'instradamento a Internet.

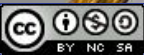


Siamo nella stessa barca

**Gli operatori di rete hanno la
responsabilità di garantire
un'infrastruttura di routing globale
robusta e sicura.**

La sicurezza della tua rete dipende da
un'infrastruttura di routing che elimina i
cattivi attori e le errate configurazioni che
causano il caos su Internet.

Più gli operatori di rete lavorano insieme,
meno incidenti ci saranno e minori saranno
i danni.



Soluzioni?

Mutually Agreed Norms for Routing Security (MANRS)

Fornisce correzioni cruciali per ridurre le più comuni minacce di routing

MANRS migliora la sicurezza e l'affidabilità del sistema di instradamento a Internet basato sulla collaborazione tra i partecipanti e sulla responsabilità condivisa dell'infrastruttura Internet.



MANRS è un passo importante da compiere

La sicurezza è un processo, non uno stato. MANRS offre una struttura e un approccio coerente per risolvere i problemi di sicurezza di Internet.

MANRS è il minimo che un operatore dovrebbe considerare, con azioni a basso rischio e convenienti.

MANRS non è una soluzione one-stop a tutti i problemi di instradamento a Internet, ma è un passo importante verso un'infrastruttura più sicura.

MANRS 4 Azioni per gli operatori

Filtraggio

Impedire la propagazione di informazioni di routing errate

Garantire la correttezza dei propri annunci e quelli dei propri clienti alle reti adiacenti con la granularità dei prefissi e degli AS-path

Anti-spoofing

Previene il traffico di indirizzi IP con origine falsificata

Abilitare la convalida dell'indirizzo di origine per almeno le reti dei clienti single-homed, i loro utenti finali e per l'infrastruttura

Coordinazione

Facilitare la comunicazione operativa globale e il coordinamento tra gli operatori di rete

Mantenere le informazioni di contatto aggiornate accessibili a livello globale nei più diffusi database di routing

Convalida globale

Facilitare la convalida delle informazioni di routing su scala globale

Pubblica i tuoi dati, così altri possono validarli



MANRS



Perché gli ISP italiani dovrebbero aderire a MANRS?

Per aiutare a risolvere i problemi della rete globale

- Dare il buon esempio per migliorare la sicurezza del routing e garantire un'infrastruttura di routing globale robusta e sicura
- Essere parte della community di MANRS può rafforzare le credenziali di sicurezza aziendale

Aggiungere valore competitivo e differenziarsi in un mercato piatto e orientato ai prezzi

- Cresce la domanda da parte dei clienti aziendali per i servizi di sicurezza gestiti
- Per segnalare competenza di sicurezza e impegno per i vostri clienti

Per trasformarsi da mero fornitore di connettività a partner di sicurezza

- I feed di informazioni e altri servizi aggiuntivi possono aumentare le entrate e ridurre i reclami dei clienti
- Le imprese mostrano una volontà di pagare di più per servizi sicuri

MANRS: chi c'è?

Attualmente solo 8 AS
italiani su oltre 1.000
dichiarano di essere
conformi a MANRS

Unisciti a noi!

Visita <https://www.manrs.org>

- Compila il modulo di iscrizione con il maggior numero di dettagli possibile.
- In risposta potremmo porre domande e testare la tua rete.

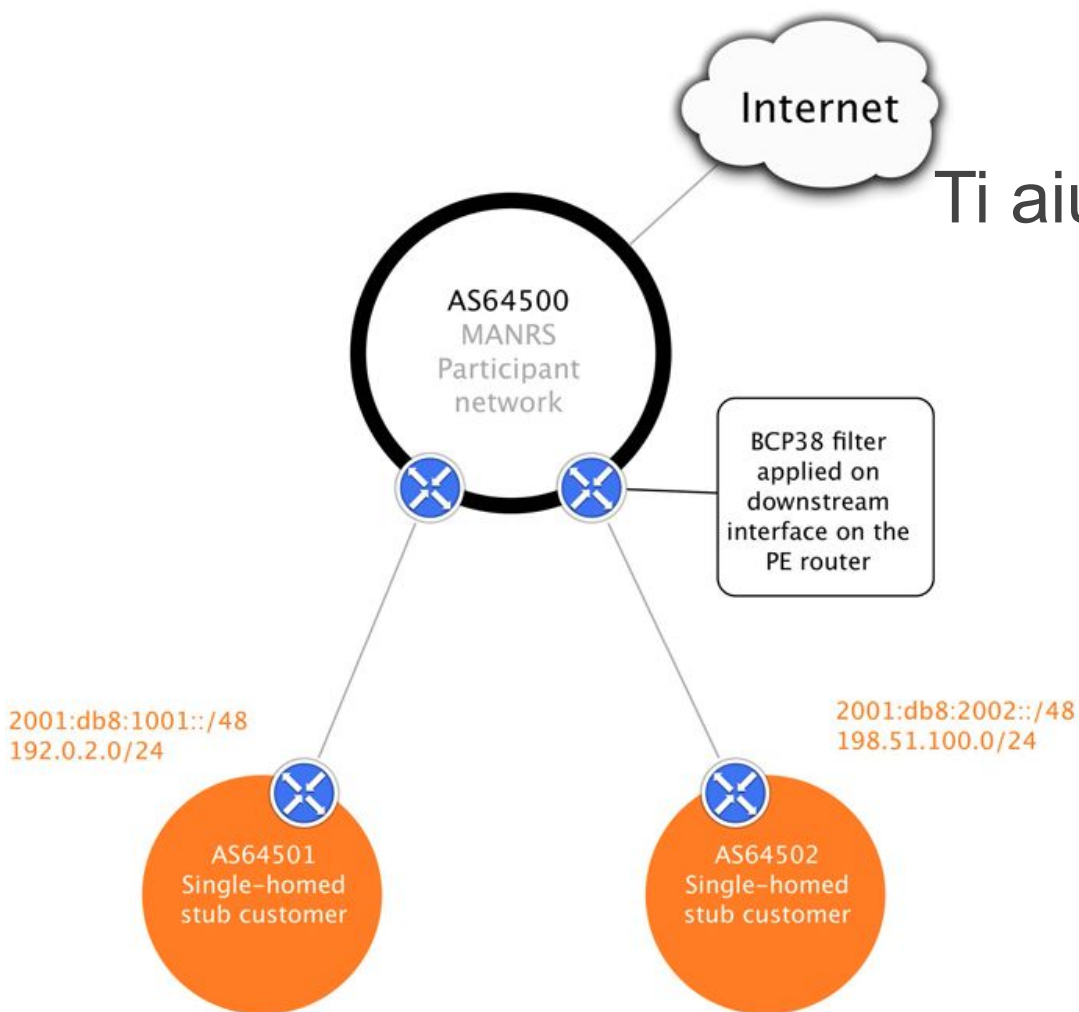
Partecipa alla community

- I membri sostengono l'iniziativa e implementano le azioni nelle loro reti
- I membri mantengono e migliorano il manifesto di MANRS e ne
- promuovono gli obiettivi



Internet

Ti aiutiamo noi



Se non sei ancora pronto a partecipare, ci sono delle linee guida per l'implementazione:

- una Guida all'implementazione basata sulle migliori pratiche operative implementate dagli operatori di rete di tutto il mondo
- 6 moduli di formazione



E poi?

Osservatorio MANRS

- Osserva lo stato effettivo di sicurezza e resilienza del sistema di routing Internet e lo traccia nel tempo.

Le misure saranno:

- Trasparenti - utilizzando dati accessibili al pubblico
- Passive: non è richiesta alcuna cooperazione dalle reti
- In evoluzione: la community di MANRS deciderà cosa viene misurato e come

Grand totals for all repositories

| | Object accepted | Manifest interval overruns certificate | certificate has expired | Policy Qualifier CPS | Stale CRL or manifest |
|--------------|-----------------|--|-------------------------|----------------------|-----------------------|
| None .cer | 5501 | | | 773 | |
| None .crl | 5496 | | | | 1 |
| None .gbr | 3 | | | | |
| None .mft | 5496 | 1 | 1 | 773 | 1 |
| None .roa | 5463 | | | 580 | |
| Total | 21959 | 1 | 1 | 2126 | 2 |

Current total object counts (distinct URIs)

| Repository | .cer | .crl | .gbr | .mft | .roa |
|------------------------|----------|----------|----------|----------|----------|
| ca.rg.net | | | | | |
| ca0.rpki.net | | | | | |
| localcert.ripe.net | | | | | |
| repository.lacnic.net | | | | | |
| rpki-pilot.lab.dtag.de | | | | | |
| rpki.afnic.net | | | | | |
| rpki.apnic.net | | | | | |
| rpki.ripe.net | | | | | |
| Total | 0 | 0 | 0 | 0 | 0 |

Overview for repository ca.rg.net

| | Object accepted | Manifest interval overruns certificate | certificate has expired | Policy Qualifier CPS | Stale CRL or manifest |
|-----------|-----------------|--|-------------------------|----------------------|-----------------------|
| None .cer | 1 | | | | |
| None .crl | 2 | | | | 1 |
| None .gbr | 1 | | | | |
| None .mft | 2 | | | | 1 |
| None .roa | 35 | | | | |

E poi?

Laboratorio pratico

Stiamo progettando un laboratorio che consentirà ai tecnici di implementare MANRS in un ambiente di rete simulato. Il laboratorio sarà disponibile:

- tramite i partner di formazione MANRS
- on-line

Se desideri ospitare l'ambiente del laboratorio di formazione MANRS, mettiti in contatto con noi! manrs@isoc.org


```
4 34288 3859237 54129 0 0 0 01w1d18h 63278
2400:bc80:1::2 4 38726 5736172 48942 0 0 0 01:11:03 Connect
2400:bc80:3::1 4 38726 6189932 48952 0 0 0 01:11:00 Connect
2400:bc80:9000::1
4 38726 2426352 48954 0 0 0 01:26:25 Connect
2402:1b80::1 4 63956 3458715 54120 0 0 0 02w4d19h 60364
2402:1b80:1000::1
4 63956 3641364 54120 0 0 0 02w4d19h 57800
```

```
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
route-views4.routeviews.org>
```

```
(config)#ipv6 route ::/0 filter ANY QUESTIONS
```