Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

GARR User Triggered Blackholing

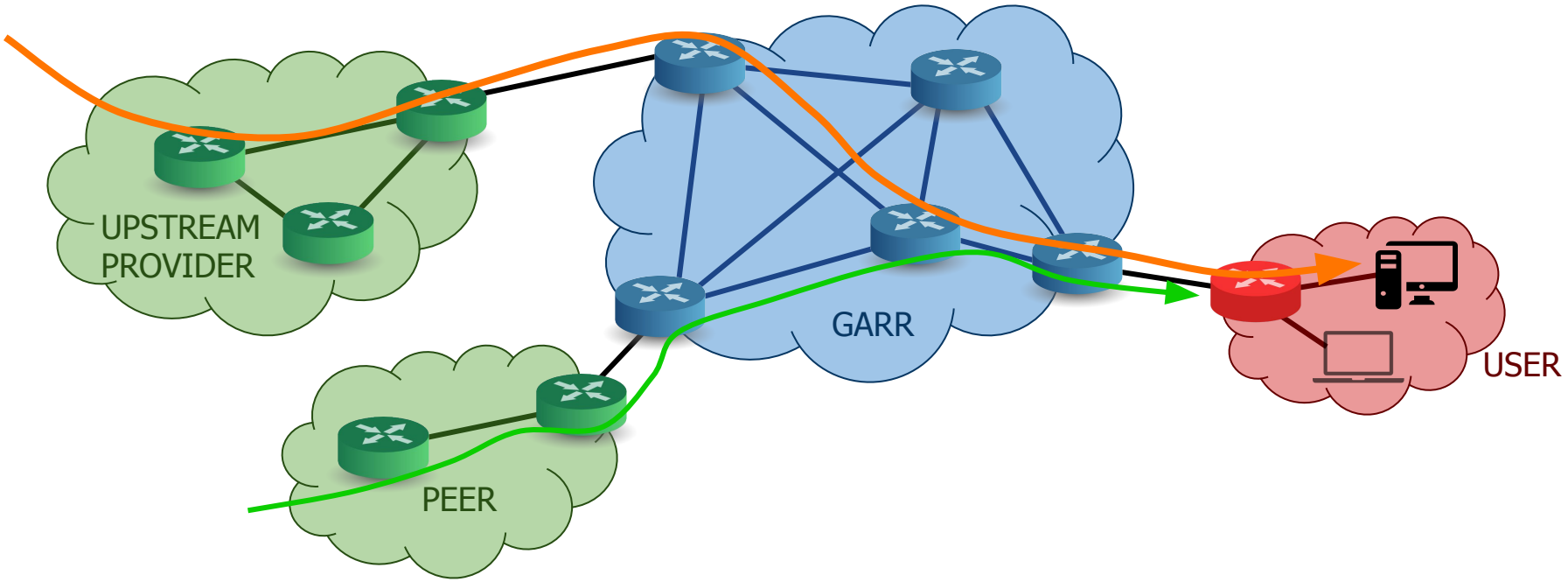
Un nuovo servizio per la comunità GARR

Silvia d'Ambrosio

Workshop GARR | Roma, 29-31/05/2018

Obiettivi del servizio

Scenario: attacco DDoS verso un host con conseguente saturazione delle risorse di rete
(della sede utente, del backbone GARR, della connessione con gli upstream provider o con i peer)



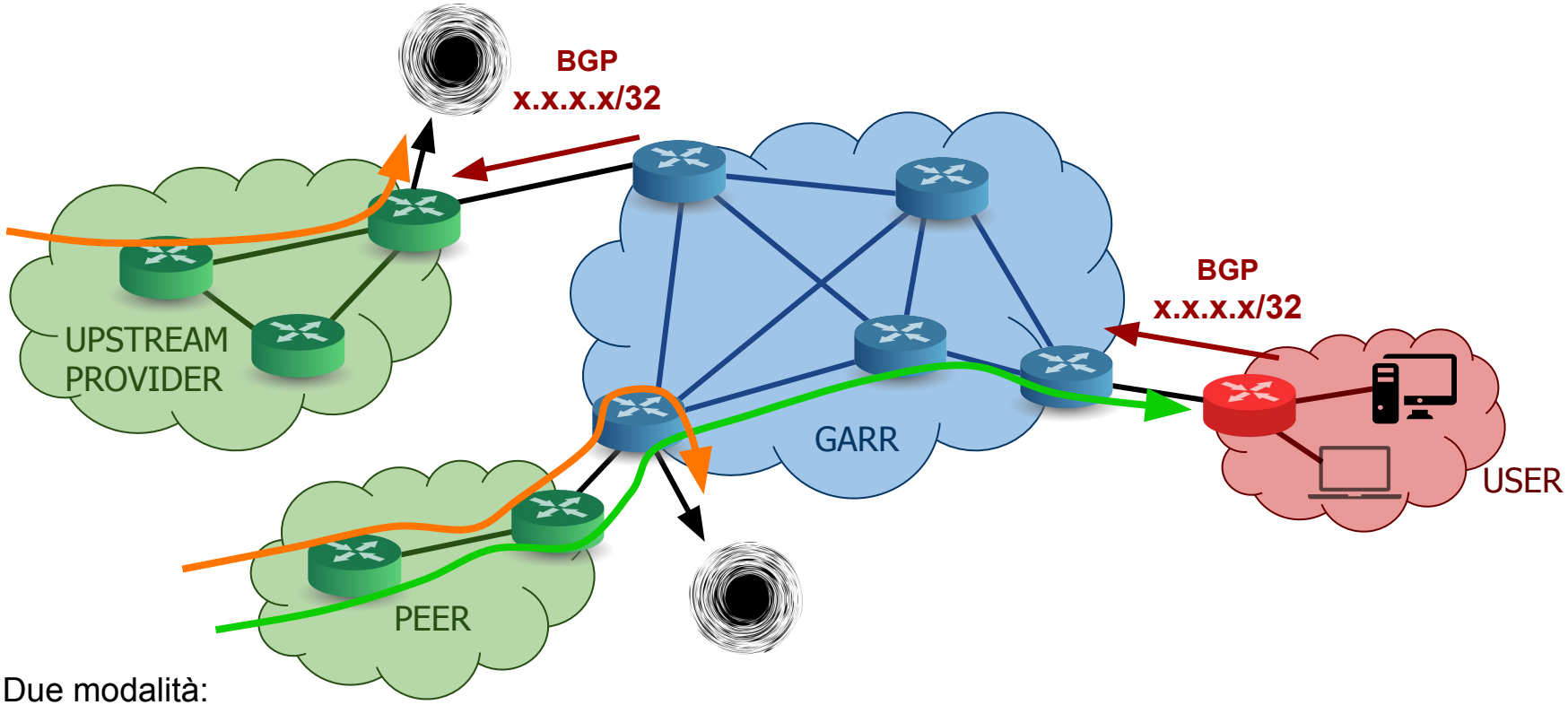
Blackholing: interruzione del traffic forwarding per una specifica destinazione da parte di un provider

- Modifica del next-hop BGP dell'IP sotto attacco per dirottare il traffico verso una null interface
- Contromisura drastica ma talvolta necessaria
- Innescato o dal Customer o dal Provider (per es. GARR)

RTBH Remote Triggered Black Hole (User driven):

- Mitigazione automatica gestita dall'APM senza esplicito intervento del GARR-NOC
- Garantire la connettività per gli host non sotto attacco
- Contromisura rapida

Architettura e Funzionamento



Due modalità:

- Blocco solo del **traffico General Internet**
  1. Annuncio BGP da parte dell'utente verso GARR per l'IP da bloccare
  2. Propagazione dell'annuncio sul backbone GARR
  3. Annuncio BGP da parte di GARR verso i provider per l'IP da bloccare

- Blocco di **tutto il traffico**
  4. Traffico scartato anche su tutti i router del backbone GARR

Implementazione del servizio

Sessione BGP:

- dove può essere configurata
  - sulla stessa sessione utilizzata per il routing o creata una sessione ad hoc
  - non obbligatoriamente sul router di frontiera
  - se possibile, anche sui link di backup

- policy in import sul router GARR
  - verificata la correttezza degli annunci

    OGNI UTENTE PUÒ RICHIEDERE IL BLACKHOLE SOLO PER GLI IP APPARTENENTI ALLA SUA LAN

  - vincolo di default per /32 (eventualmente permesse subnet più ampie)

Annuncio BGP da parte dell'utente:

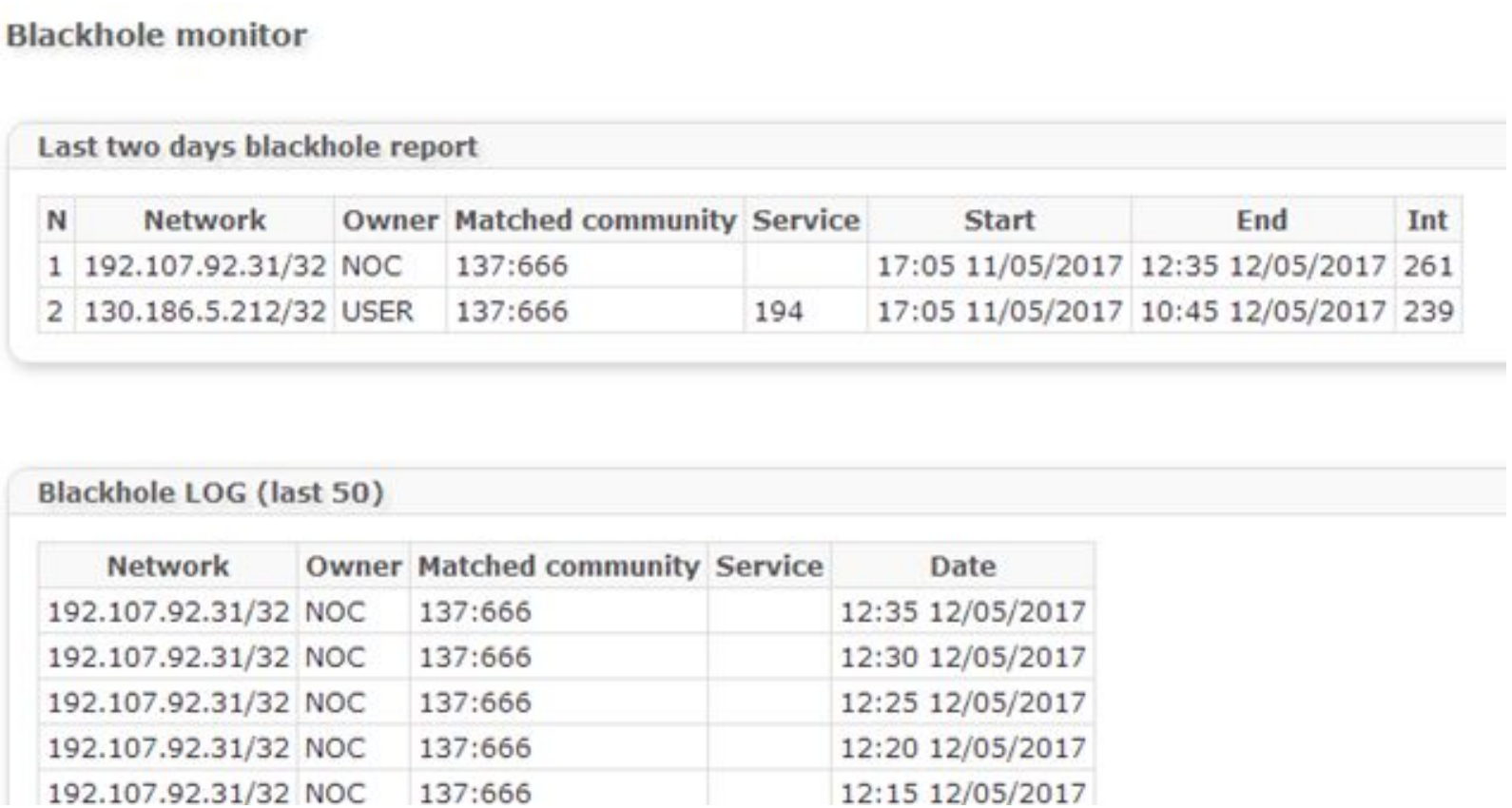
- selezione delle modalità
  - community 666: blackhole su upstream provider e backbone GARR
  - community 667: blackhole solo su upstream provider

- configurazione e disabilitazione
  - manualmente
  - automaticamente (per esempio sfruttando FastNetMon ed exaBGP)

- responsabilità dell'utente

Monitoring e Ticketing

Blackhole monitor: Tool interno per il monitoraggio delle mitigazioni effettuate



Blackhole monitor

Last two days blackhole report

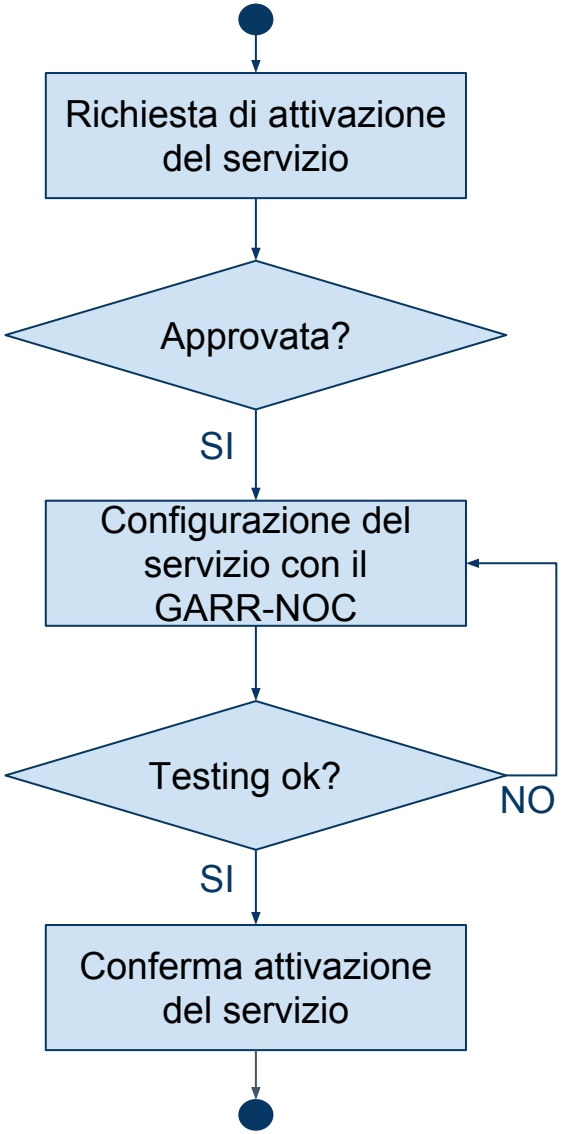
N	Network	Owner	Matched community	Service	Start	End	Int
1	192.107.92.31/32	NOC	137:666		17:05 11/05/2017	12:35 12/05/2017	261
2	130.186.5.212/32	USER	137:666	194	17:05 11/05/2017	10:45 12/05/2017	239

Blackhole LOG (last 50)

Network	Owner	Matched community	Service	Date
192.107.92.31/32	NOC	137:666		12:35 12/05/2017
192.107.92.31/32	NOC	137:666		12:30 12/05/2017
192.107.92.31/32	NOC	137:666		12:25 12/05/2017
192.107.92.31/32	NOC	137:666		12:20 12/05/2017
192.107.92.31/32	NOC	137:666		12:15 12/05/2017

TTS NOC-CERT: sistema di ticketing interno per tenere traccia degli attacchi DDoS riscontrati

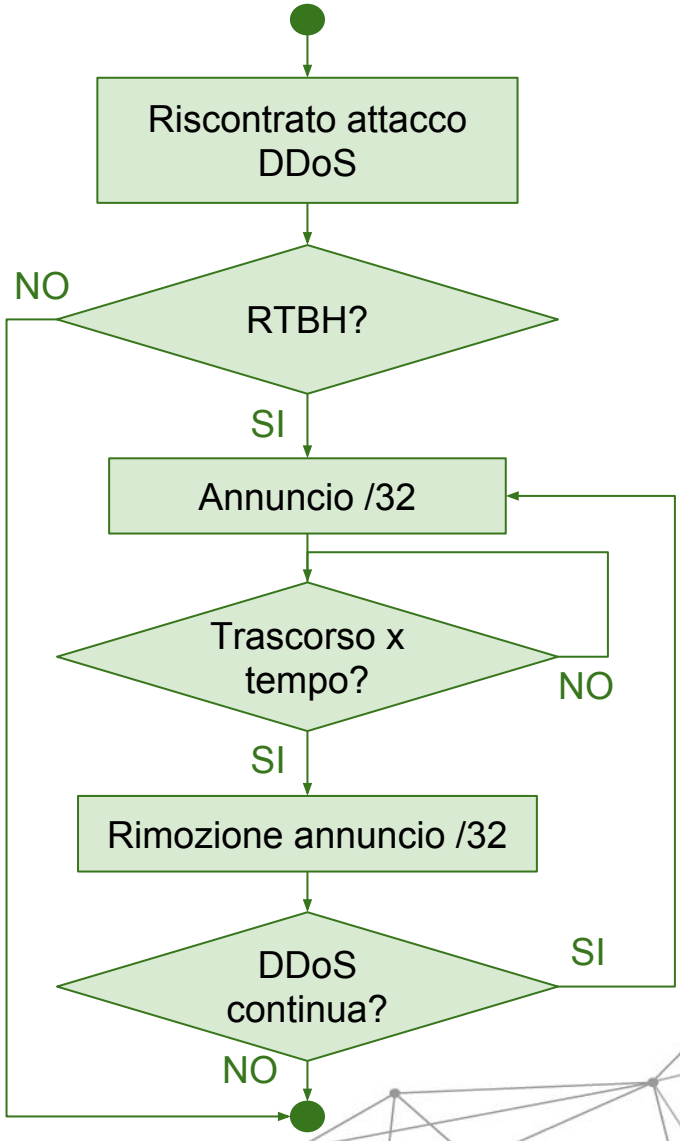
Procedure per gli APM: attivazione del servizio



- La richiesta di attivazione del servizio può essere effettuata dall'APM per e-mail scrivendo a planning@garr.it, inserendo in copia esplicita l'APA e noc@garr.it
- L'APM riceverà una mail di approvazione dal gruppo planning di GARR
- Il GARR-NOC e l'APM si accorderanno sui dettagli specifici inerenti l'implementazione del servizio. La configurazione verrà effettuata in finestra di manutenzione programmata con il supporto del GARR-NOC
- In finestra di manutenzione saranno effettuati anche tutte le opportune verifiche per testare il corretto funzionamento del servizio
- Il GARR-NOC confermerà tramite e-mail ad APA ed APM l'avvenuta attivazione del servizio richiesto

Procedure per gli APM: servizio in produzione

- L'APM si accorge di essere vittima di un attacco DDoS ed effettua un'analisi dell'attacco
- L'APM valuta se usufruire della funzionalità' di RTBH o effettuare un altro tipo di mitigazione (per esempio un filtro sul firewall utente)
- L'APM configura l'annuncio BGP per l'indirizzo IP da bloccare, con l'opportuna community, e lo comunica al GARR-NOC tramite e-mail
- Trascorso un intervallo di tempo prestabilito (per esempio 30 minuti), l'APM rimuove l'annuncio BGP e informa il GARR-NOC tramite e-mail
- L'APM verifica il termine dell'attacco DDoS, chiedendo eventualmente riscontro al GARR-NOC. Qualora dovesse ripresentarsi l'attacco, si suggerisce di applicare nuovamente il blackholing impostando un intervallo temporale via via crescente, ma non illimitato (ad esempio 1h, 2h, 6h, 12h...)



Documenti e Sviluppi futuri

Documenti:

- presentazione disponibile sul sito del workshop www.eventi.garr.it/it/ws18
- documento pdf a breve disponibile sul sito GARR-NOC www.noc.garr.it
- RFC 3882 ed RFC 7999

Sviluppi futuri:

- **Flowspec**: utilizzo del BGP per propagare specifiche regole di filtraggio
- **Scrubbing Center**: utilizzo del BGP per inoltrare l'attacco verso una macchina di ripulitura del traffico

Grazie