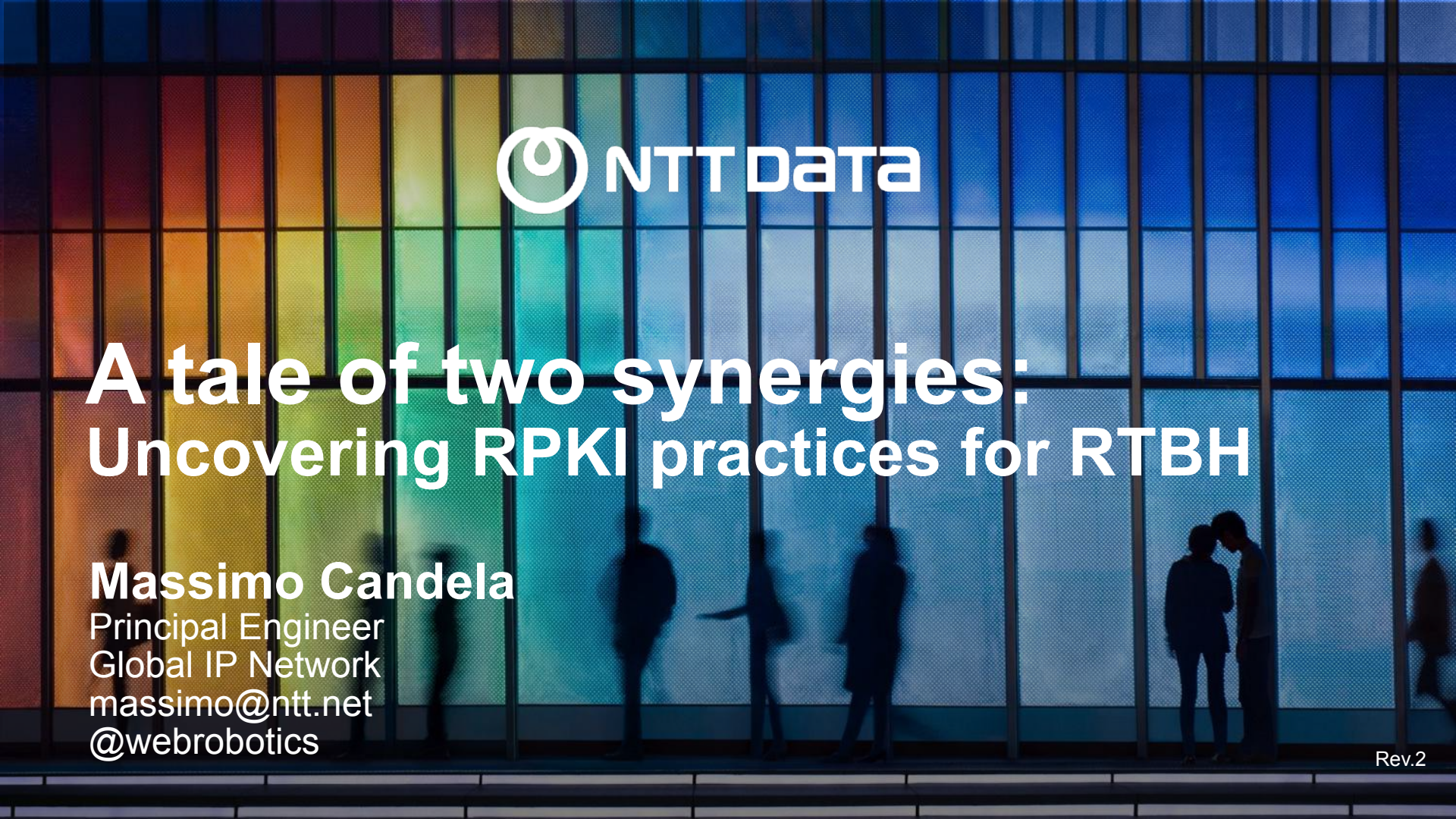


A tale of two synergies:
Uncovering RPKI practices for RTBH

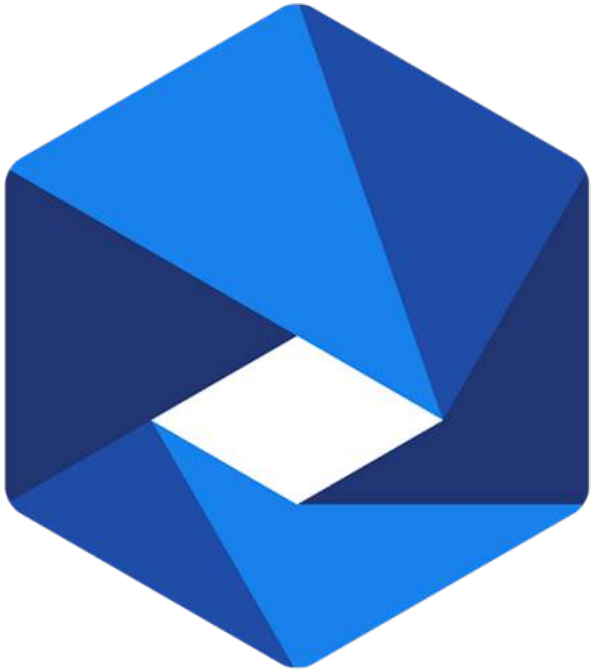
Massimo Candela
Principal Engineer
Global IP Network
massimo@ntt.net
@webrobotics

Rev.2

Co-authors

Ioana Livadariu (SimulaMet)
Romain Fontugne (IIJ)
Amreesh Phokeer (ISOC)
Massimiliano Stucchi (AS58280)

MANRS



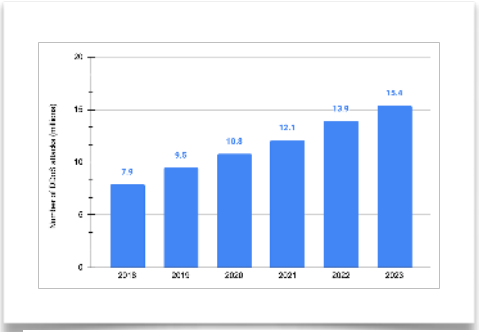
- Mutually Agreed Norms for Routing Security
- A list of concrete actions for ISPs, IXPs, CDNs, and HW vendors

DDoS and BGP Hijacks

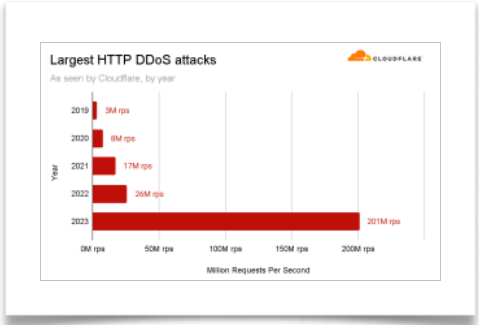
- DDoS
  - A Distributed Denial of Service aims at overwhelming the target network/service
- BGP Hijack
  - A BGP hijack aims at rerouting traffic where it was not supposed to go

DDoS and BGP Hijacks

- DDoS

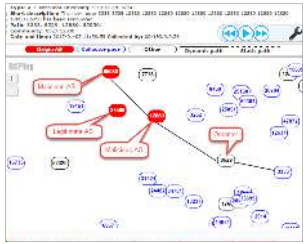


Number of DDoS attacks *- Cisco Annual Internet Report*



Largest HTTP DDoS attacks *- Cloudflare*

- BGP Hijack



Massimo Candela | massimo@ntt.net | @webrobotics

DDoS and BGP Hijacks - Mitigation

- DDoS
  - A Distributed Denial of Service aims at overwhelming the target network/service
  - **Mitigation:**
    - **Remotely Triggered Black Hole (RTBH)**

- BGP Hijack
  - A BGP hijack aims at rerouting traffic where it was not supposed to go
  - **Mitigation:**
    - **Resource Public Key Infrastructure (RPKI)**

Massimo Candela | massimo@ntt.net | @webrobotics

DDoS and BGP Hijacks - Mitigation

- RTBH
  - A network operator target of a DDoS attack can propagate a BGP update with specific BGP communities or next-hop IP to instruct peers to drop the malicious traffic
- RPKI
  - A hijack affecting a prefix for which a Route Origin Authorization (ROA) exists will be ineffective on networks operating Route Origin Validation (ROV)

RTBH at NTT

Blackhole and Selective Blackhole service

Customers may announce hosts tagged with 2914:666 for v4 and v6 peering. Any /32 or /128 host tagged with this community will be discarded as soon as it reaches our network. The /32 or /128 prefix must be one included in the customer's existing ingress BGP filter. By default, peers are not configured for the blackhole functionality. Please contact the NTT NOC @ **noc@gin.ntt.net** for this feature.

As of the beginning of March, 2015, NTT now offers Selective Blackholing. This provides the ability to limit the scope of the blackholing to certain geographic locations, allowing a more strategic application of the blackhole service.

Selective Blackhole communities	
2914:661	only blackhole inside the region the announcement originated
2914:663	only blackhole inside the country the announcement originated
2914:660	only blackhole outside the region the announcement originated
2914:664	only blackhole outside the country the announcement originated

More at: https://www.gin.ntt.net/support-center/policies-procedures/routing/

DDoS protection at NTT

- We offer also a DDoS protection service
  - https://www.gin.ntt.net/products-services/network-security/ddos-protection-services/
  - Rerouting, scrubbing
  - You can chose to trigger it manually or automatically (auto-detection)
  - Can be used to protect yourself or your customers

RTBH and RPKI

- RTBH
  - A network operator target of a DDoS attack can propagate a BGP update with specific BGP communities or next-hop IP to instruct peers to drop the malicious traffic
- RPKI
  - A hijack affecting a prefix for which a Route Origin Authorization (ROA) exists will be ineffective on networks operating Route Origin Validation (ROV)

Problem: A RTBH request can be RPKI invalid

Massimo Candela | massimo@ntt.net | @webrobotics

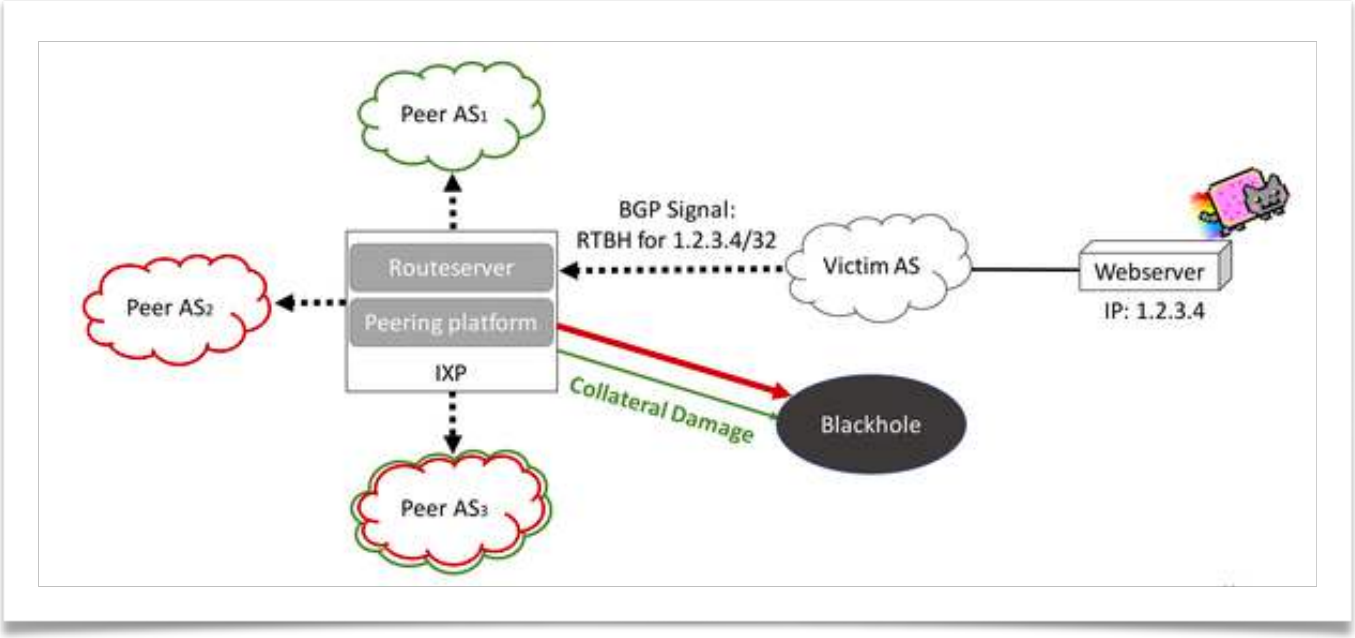
RPKI + RTBH and the time dimension

- Most RTBH are about /32 (/128)
- /32 and /128 are usually not covered by ROAs
  - But a less-specific prefix can be! (**RPKI invalid**)
- RPKI has a publication and propagation time
  - See https://www.youtube.com/watch?v=LEDDXTyoHTM
  - See https://ripe88.ripe.net/archives/video/1384/
  - Read https://manrs.org/2023/03/tracking-time-delays-in-the-rpki-based-route-origin-validation-supply-chain/

DDoS mitigation needs a fast response not compatible with RPKI timings

Massimo Candela | massimo@ntt.net | @webrobotics

RTBH at IXP



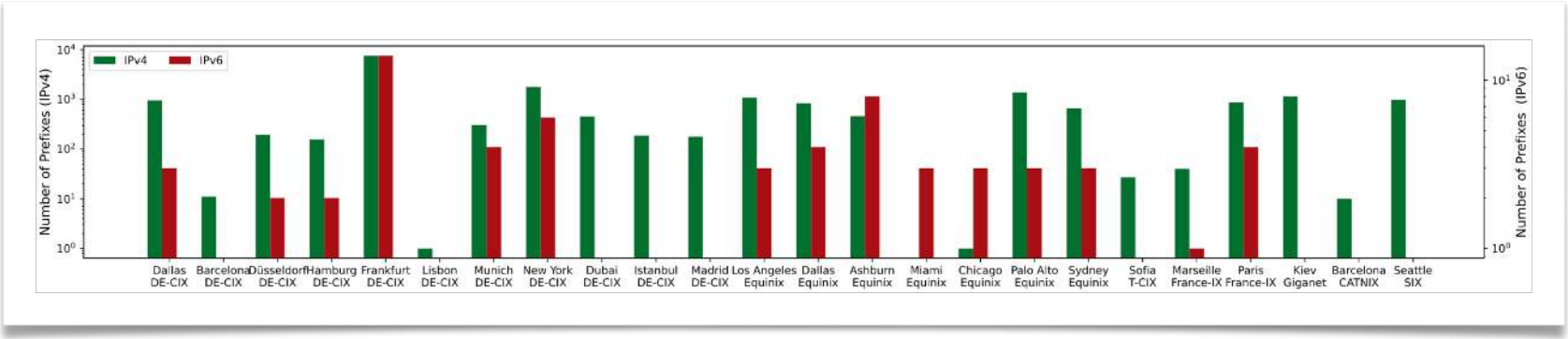
Remote Triggered Black Hole filtering - *APNIC Blog*

PCH (BGP) and RIPE (RPKI)

- Packet Clearing House (PCH) collects BGP data from over 300 Internet Exchange Points (IXPs)
- We use their MRT files to look for RTBH requests

- The RIPE RPKI historical dataset contains records of Route Origin Authorizations (ROAs)
- We use it for historical RPKI validation

RTBH at IXP

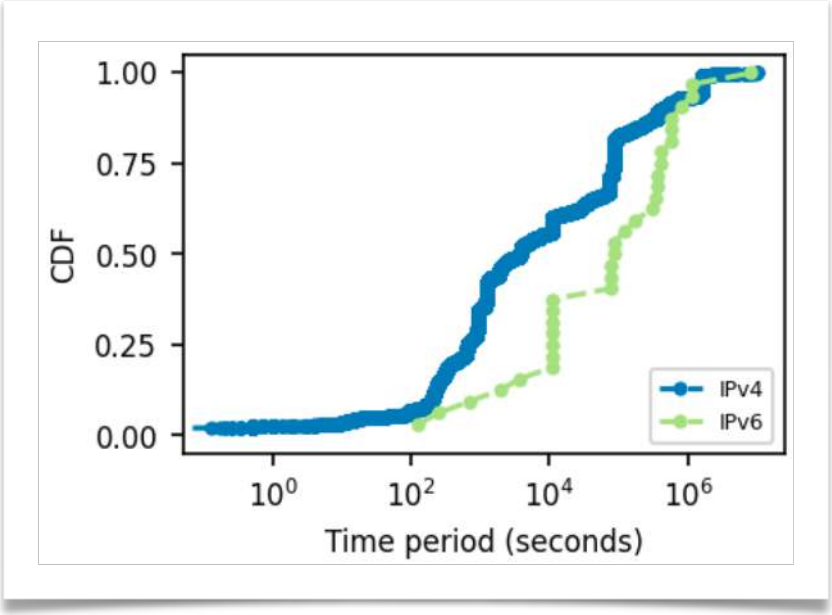


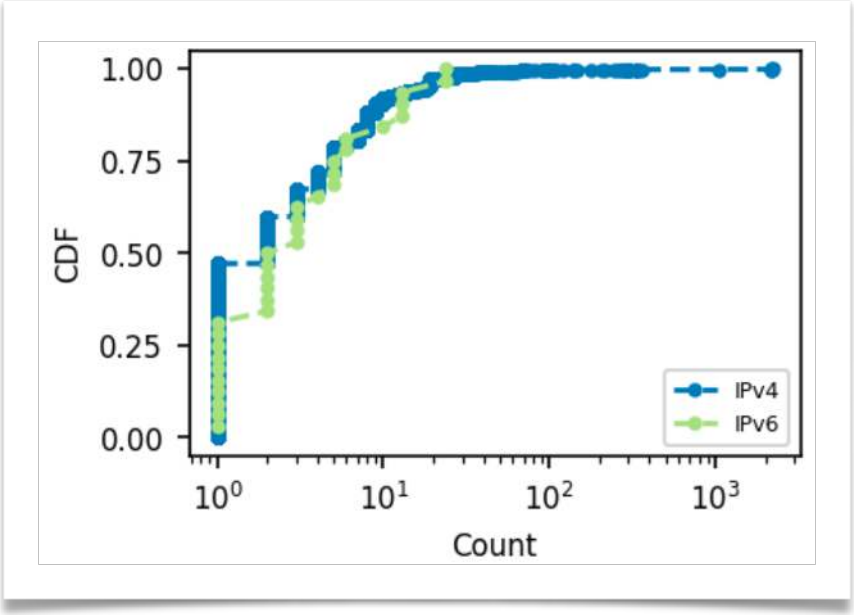
Number of IPv4 and IPv6 prefixes blackholed at the PCH BGP collectors

- Blackholed 12K IPv4 and 32 IPv6 prefixes by 225 peers across 24 IXPs
- **Most of the blackholed prefixes are /32 and /128**

Massimo Candela | massimo@ntt.net | @webrobotics

RTBH duration and count



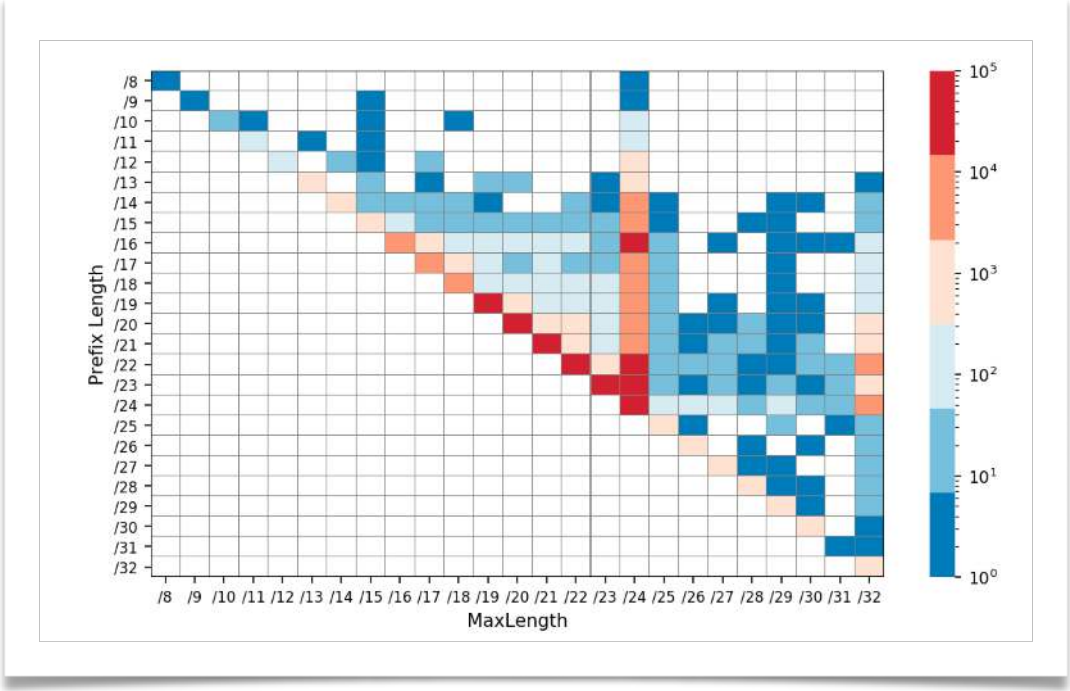


- Duration (seconds) of a blackhole
- Count of times the same prefix is blackholed in the observed period

Massimo Candela | massimo@ntt.net | @webrobotics

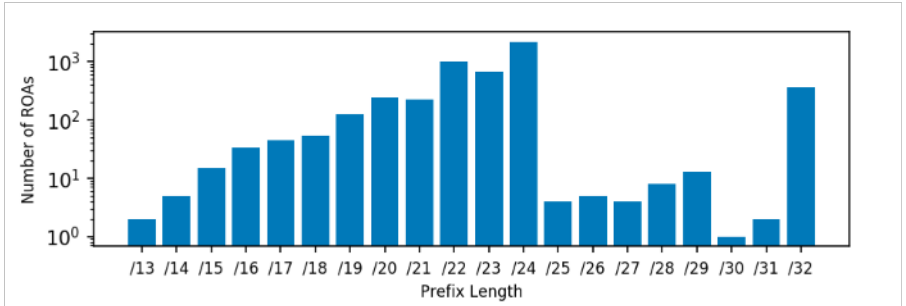
RPKI deployment and MaxLength

- PrefixLength **equals** MaxLength in 82.6% (IPv4) and 86.8% (IPv6) of the ROAs
  - *The remaining may still be vulnerable to hijacks*

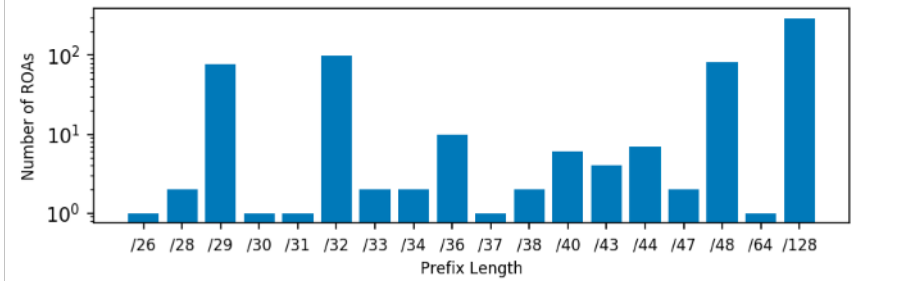


Massimo Candela | massimo@ntt.net | @webrobotics

RPKI deployment and MaxLength



(a) ROAs for IPv4 prefixes



(b) ROAs for IPv6 prefixes

Fig. 5: Number of ROAs with *maxLength* is equal to (a) /32 and (b) /128.

- What's the prefix length of ROAs with 32 (128) MaxLength?

Massimo Candela | massimo@ntt.net | @webrobotics

RPKI attitude peers involved in RTBH

- **RPKI-strict:** RTBH affected prefixes are covered by dedicated ROAs
- **RPKI-loose:** RTBH affected prefixes are covered by ROAs with wider MaxLength
- **RTBH-agnostic:** RTBH affected prefixes are RPKI invalid

Operator Profile	*IPv4*	*IPv6*
RPKI-strict	4	1
RPKI-loose	26	1
RTBH-agnostic	182	6

Number of IXP peers -involved in RTBH - grouped by RTBH+RPKI attitude

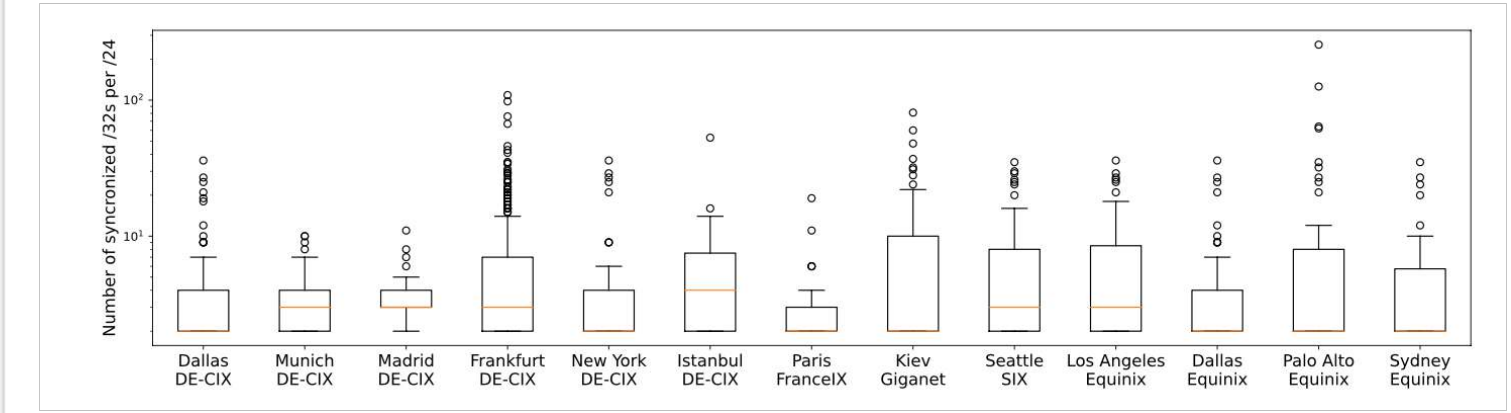
Massimo Candela | massimo@ntt.net | @webrobotics

RPKI + RTBH how often?

- **~91%** of IXP members that do RTBH also register ROAs
  - RPKI+RTBH is quite common
  - 85% of the operators sent RPKI invalid RTBH requests

/32 of /24? (synchronized in time)

- 1/3 of the blackholed /32s are isolated
- Many /32 blackholed in pairs in same /24
- There are outliers of 100+ /32 of belonging to the same /24 being blackholed



Conclusions

- ~10% of the IXP members use RTBH
- Most of the blackholed prefixes are /32s (/128s) for IPv4 (IPv6) prefixes for ~short periods of time
- ~20% of the operators deploy RPKI wrongly and remain potentially vulnerable to hijacks
- ~91% of the operators that trigger blackholes also register ROAs
- ~85% of the operators sent RPKI invalid RTBH requests
  - ISPs place their trust in IXPs making exceptions to ROV for RTBH requests
  - ISPs place their trust in other peers to accept these requests

Massimo Candela | massimo@ntt.net | @webrobotics

Thank you.

Massimo Candela
Principal Engineer, Network Information Systems Development
Global IP Network
massimo@ntt.net
@webrobotics

www.gin.ntt.net
@GinNTTnet #globalipnetwork #AS2914