24 October 2022

MANRS BCOP Topics

BCOP Task Force Meeting @ RIPE 85

Kevin Meynell
Senior Manager, Technical & Operational Engagement
meynell@isoc.org

Agenda

1) **Bogons, definition, operational practices and MANRS conformance** – Kevin Meynell (ISOC)

2) **MANRS+** – Andrei Robachevsky (ISOC)

3) **MANRS conformance tools & documentation** – Andrei Robachevsky & Max Stucchi (ISOC)

Bogons, definition, operational practices and MANRS conformance

Kevin Meynell <meynell@isoc.org>

A bit of history…

Term derived from Hitchhikers Guide to the Galaxy

Vogons – who were “not known to be helpful” - mispronounced as ‘bogons’ by Arthur Dent

First appeared in networking in 1983 (as synonym for *bogus*)

Informal term with no definitive definition

Officially described as *Reserved* addresses by RIRs

What is a bogon?

Team Cymru definition

A bogon prefix is a route that should never appear in the Internet routing table.

What is a bogon?

Geoff Huston definition

In the context of the Internet address realm, a bogon refers to the use of an address or, more generally a route object, that is not duly authorized by the entity to which the address, or resource, was originally assigned.

What is a bogon?

RFC 3871 definition

A "Bogon" (plural: "bogons") is a packet with an IP source address in an address block not yet allocated by IANA or the Regional Internet Registries (ARIN, RIPE, APNIC...) as well as all addresses reserved for private or special use by RFCs.

What is a bogon?

Erm… MANRS definition

An ASN or IP Prefix that is not allocated by IANA or an RIR, or is a Special Purpose Address as defined by RFC 6890. These should not be routed on the Internet.

So what's the problem?

The Border Gateway Protocol (BGP) used by the Internet routing system is based entirely on *unverified trust* between networks

- No built-in validation that updates are legitimate
- Any network can announce any ASN or IP prefix
- Any network can claim to be another network

MANRS

MANRS: Mutually Assured Norms for Routing Security

- Aims to eliminate the most common threats in the global routing system
- Brings together established industry best practices
- Measures the state of global routing security – https://observatory.manrs.org

Filtering

Prevent propagation of incorrect routing information

Ensure the correctness of your own announcements and announcements from your customers to adjacent networks with prefix and AS-path granularity

Anti-spoofing

Prevent traffic with spoofed source IP addresses

Enable source address validation for at least single-homed stub customer networks, their own end-users, and infrastructure

Coordination

Facilitate operational communication and coordination between network operators

Maintain globally accessible up-to-date contact information in relevant RIR database and/or PeeringDB

Global Validation

Facilitate validation of routing information

Publish your routing data, so others can validate

Registering number resources in an IRR and/or creating ROAs for them

MONTH September 2022

USE GRIP DATA

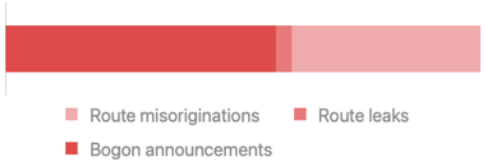
Overview

State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

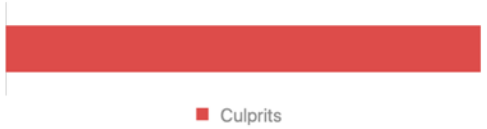
Incidents

Route misoriginations	626
Route leaks	53
Bogon announcements	897
Total	1,576



Culprits

Culprits	1,110

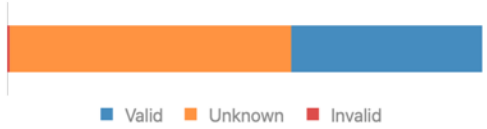


Routing completeness (IRR)

Unregistered	133,906	11.9%
Registered	987,031	88.1%

Routing completeness (RPKI)

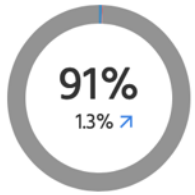
Valid	450,331	40.2%
Unknown	664,639	59.3%
Invalid	5,967	0.5%



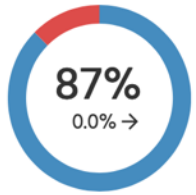
MANRS Readiness

Filtering

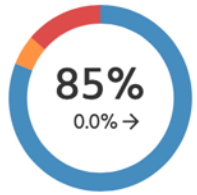
Anti-spoofing



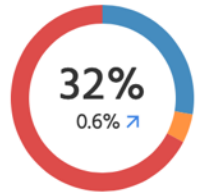
Coordination



Global Validation IRR



Global Validation RPKI



Ready Aspiring Lagging No Data Available

M3 - Bogon prefixes announced by the AS

Absolute: **31.0** Normalized: **17%** Incident Count: **1**

Incident Id: 1 Absolute: 31.0 Start Date: 01-09-2022 01-00-00 End Date: 01-10-2022 01-00-00 Duration: 30d, 0m, 0s

Incident Id	Start Time	End Time	Prefix	Paths	Weight	Source
1	2022-09-01 00:00:00	2022-10-01 00:00:00	41.78.60.0/22	Paths	1	cidr
1	2022-09-01 00:00:00	2022-10-01 00:00:00	208.84.80.0/21	Paths	1	cidr

Download metrics data

M3C - Bogon prefixes propagated by the AS

Absolute: **31.0** Normalized: **17%** Incident Count: **1**

Incident Id: 1 Absolute: 31.0 Start Date: 01-09-2022 01-00-00 End Date: 01-10-2022 01-00-00 Duration: 30d, 0m, 0s

Incident Id	Start Time	End Time	Prefix	Paths	Weight	Source
1	2022-09-01 00:00:00	2022-09-24 00:00:00	41.205.225.0/24	Paths	1	cidr
1	2022-09-01 00:00:00	2022-10-01 00:00:00	103.98.77.0/24	Paths	1	cidr
1	2022-09-01 00:00:00	2022-10-01 00:00:00	162.211.248.0/22	Paths	1	cidr
1	2022-09-01 00:00:00	2022-10-01 00:00:00	190.3.166.0/23	Paths	1	cidr
1	2022-09-01 00:00:00	2022-09-07 00:00:00	41.205.233.0/24	Paths	1	cidr
1	2022-09-01 00:00:00	2022-09-24 00:00:00	41.205.238.0/24	Paths	1	cidr
1	2022-09-01 00:00:00	2022-09-21 00:00:00	209.161.123.0/24	Paths	1	cidr
1	2022-09-01 00:00:00	2022-09-21 00:00:00	209.161.127.0/24	Paths	1	cidr

To summarise…

A bogon is an IP address that should not be routed on the public Internet

Bogon advertisements constitute around 50% of observed route incidents

Not as bad as a route leak or hijack - not using someone else's resources (in theory) - but should still be identified and filtered

Okay, but we should be able to identify the bogons, right?

- NRO publishes number resource delegated stats daily
- Special Purpose addresses are defined in RFC 6890
- CIDR report generates bogon lists - https://www.cidr-report.org/as2.0/#Bogons

Err, no – we have the administrative bogon issue

An administrative bogon (a MANRS-defined term) is a number resource legitimately assigned to an operator, but which has been marked bogon by a RIR for administrative reasons – typically loss of contact or unpaid bill

Normally marked bogon for a short period and thereafter reverts to assigned

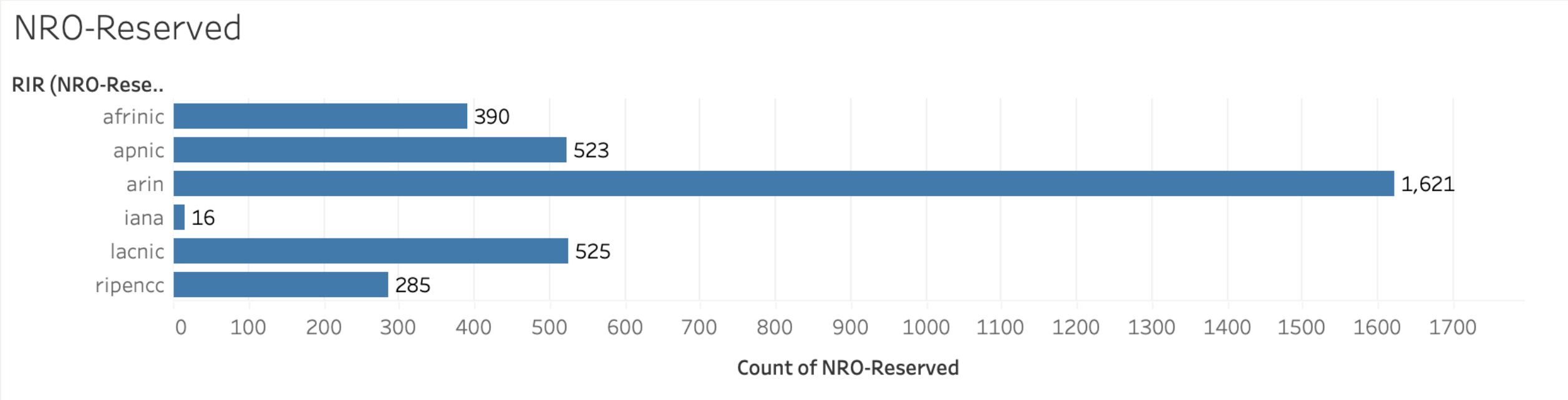
RIRs do not distinguish between different types of bogons

RIRS policies on marking number resources bogon are all different and not published

Administrative bogons constitute 80% of all bogons (and 40% of all route incidents)

Causing significant problems with measuring route incidents and therefore conformance with routing security best practice

NRO Delegation File – Reserved [3360]



https://ftp.ripe.net/pub/stats/ripencc/nro-stats/latest/nro-delegated-stats

MANRS

How do we solve the problem?

We need to exclude administrative bogons from routing conformance measurement:

- Makes accurate measurement more difficult
- Reduces routing security assurances (e.g. MANRS Action 1)
- Makes ROV and dropping of invalid routes more problematic (technically and legally)

Optimal solution = support from RIRs to categorise different types of bogons:

- We're not interested in the reason why number resources are marked bogon
- Different per-RIR transitional periods for categorisation is acceptable
- RIRS are the definitive source of truth on the status of number resources

MANRS

Best Practice questions

Should there be a standard way of marking a bogon for routing security purposes?

- Should administrative bogons be included in overall route incident statistics (i.e. only excluded from individual ASN conformance scores)?
- How long before an administrative bogon should become a ‘full’ bogon?
- Should administrative bogons be marked as bogon at all (would require policy changes)?

Proposed NRO Communique

NRO Communique

The Mutually Agreed Norms for Routing Security (MANRS) is a global initiative whose aim is to help reduce the incidence and impact of well-known inter-domain routing threats.

Part of our mission is to measure compliance of participating organizations to the actions specified in each MANRS programme. This measurement requires that we determine whether a network is originating or advertising address prefixes which are not assigned or allocated by RIRs.

Measurement is a precise activity, and we have found that due to subtle differences in how each of the five RIRs handles registration, deregistration and registration changes, it is difficult to determine how to definitively classify the state of a number resource. As such, we request the Regional Internet Registries, coordinated by the NRO, establish precise and shared definitions of the terms used to describe the various states that a number resource can be in.

Last but not least…

MANRS Community Meeting

Tuesday, 25 October 2022 @ 12.30-14.00

MANRS Steering Committee elections

Nominations open until 28 October 2022

https://www.manrs.org/2022/10/nominations-open-for-manrs-steering-committee/

MANRS+

Benefits

- MANRS+ organizations would have access to a special certification or quality mark, gaining competitive advantage in the marketplace and therefore reinforcing the value of MANRS
- Business partners would recognize the MANRS+ certification or quality mark, preferring or requiring it in procurement processes and assuring the services they provide adhere to routing security best practices

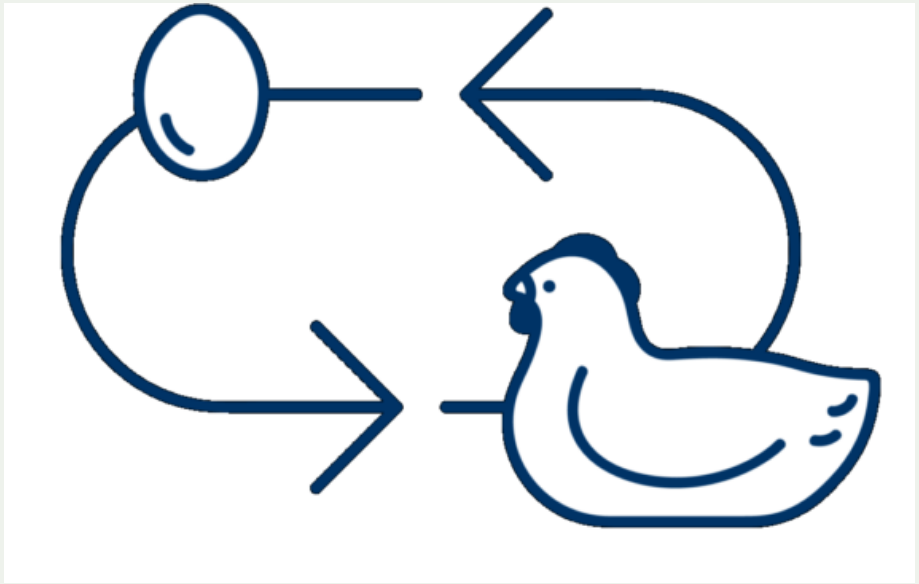
Development Challenges

- Customer requirements that will add value for them are not well known (also to the customers themselves). This aspect of security and the nature of transitive risk is often not in the focus.
- Transparent and credible audit for each of the controls is a key. It cannot be too costly and should be automated as much as possible
- Incremental approach, filling in the general framework with building blocks

Source: https://www.vecteezy.com/members/lizfa

Implementation Challenges

- Mutual dependency: MANRS+ participants will not invest in more stringent requirements without a compelling business case, and organizations will not require a MANRS Plus quality mark if it is not a well-recognized industry standard.
- We must take care not to alienate or confuse existing MANRS participants and explain the new tiered options thoughtfully and clearly.



MANRS+ WG Charter: the Goals

1. Solicit input potential consumers of the mark to identify a viable set of security requirements for connectivity providers (network transit providers) that has additional value to customers.
2. Based on collected input, develop an expanded set of MANRS Actions for network operators, CDNs, and Cloud providers.
3. Develop requirements for conformance testing of the Actions.
4. Identify requirements for necessary tooling for conformance testing and other aspects of the quality mark.
5. Identify potential partners for the development of a certification program for MANRS+ .

MANRS Documentation

MANRS Documentation

- New github repository for the MANRS Documentation
  - 2 Docs at the moment:
    - Network Implementation guide
    - IXP Implementation guide
- Any contribution is welcome
  - Documents are in Markdown
  - Send a pull request or get in touch with us

https://github.com/manrs-tools/manrs-docs/