
INTERNET2
2022
TECHNOLOGY
exchange
A New MANRS Program for the R&E Community
Andrew Gallo
INTERNET2

What is MANRS?

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats. MANRS offers specific actions via four programs for Network Operators, Internet Exchange Points, CDN and Cloud Providers, and Equipment Vendors.

A bit of history

- In 2014, a group gathered to improve the security and resilience of the global routing system
- Produced ***Routing Resilience Manifesto***
- Original contributors
  - David Freedman, *Claranet*
  - Wesley George, *Time Warner Cable*
  - Jason Livingood, *Comcast*
  - Andrei Robachevsky, *Internet Society*
  - Job Snijders, *NTT*
  - Tony Tauber, *Comcast*

MANRS Today

- MANRS is a collaborative initiative of Internet operators
- The MANRS Participants are the Internet operators that meet the requirements of the (currently) 4 MANRS programmes:

  Network Operators – 746 participants (899 ASNs)

  IXPs – 107 participants

  CDN/Cloud Providers – 22 participants

  Vendors – 6 participants

MANRS Steering Committee

- The Internet Society has developed and supported the MANRS initiative, which has grown quickly and also gained credibility outside of the operator community
- MANRS has become bigger than what ISOC staff can support alone
- Increasing number of decisions also need to be made :
  - Auditing questions as they arise
  - How to strengthen the existing MANRS Actions
  - Development of ongoing MANRS conformance criteria
  - How to handle participants failing to meet the necessary criteria for MANRS conformance
  - Development of new programmes

- **MANRS should be a self-regulating community!**

MANRS Steering Committee Membership

Elections were held on November 2022, and following persons were elected:

- Warrick Mitchell (***AARNet***) – Chair, until 31 October 2024
- Andrew Gallo (***GWU***) – Deputy-Chair, until 31 October 2024
- Flavio Luciani (NAMEX) – until 31 October 2024
- Nick Hilliard (INEX) – until 31 October 2023
- Arnold Nipper (DE-CIX) – until 31 October 2023
- Arturo Sevrin (Google) – until 31 October 2023
- Melchior Aelmans (Juniper) - until 31 October 2025
- Musa Stephen Honlue (AFRINIC) – until 31 October 2025
- Tony Tauber (Comcast) – until 31 October 2025

MANRS Auditing Officers

Hanna Kreitem (ISOC)
Kevin Meynell (ISOC)
Andrei Robachevsky (ISOC)
Aftab Siddiqui (ISOC)
Ashlyn Witter (ISOC)

R&E is well represented!

Some Recent Security Incidents

- Vodafone leaks >30 prefixes
- Rostelecom announces prefixes of Akami, Cloudflare, AWS...
- AWS Route53 DNS prefixes Hijacked, MyEtherWallet users targetted
- Two Million in Cryptocurrency stolen from KLAYSwap users

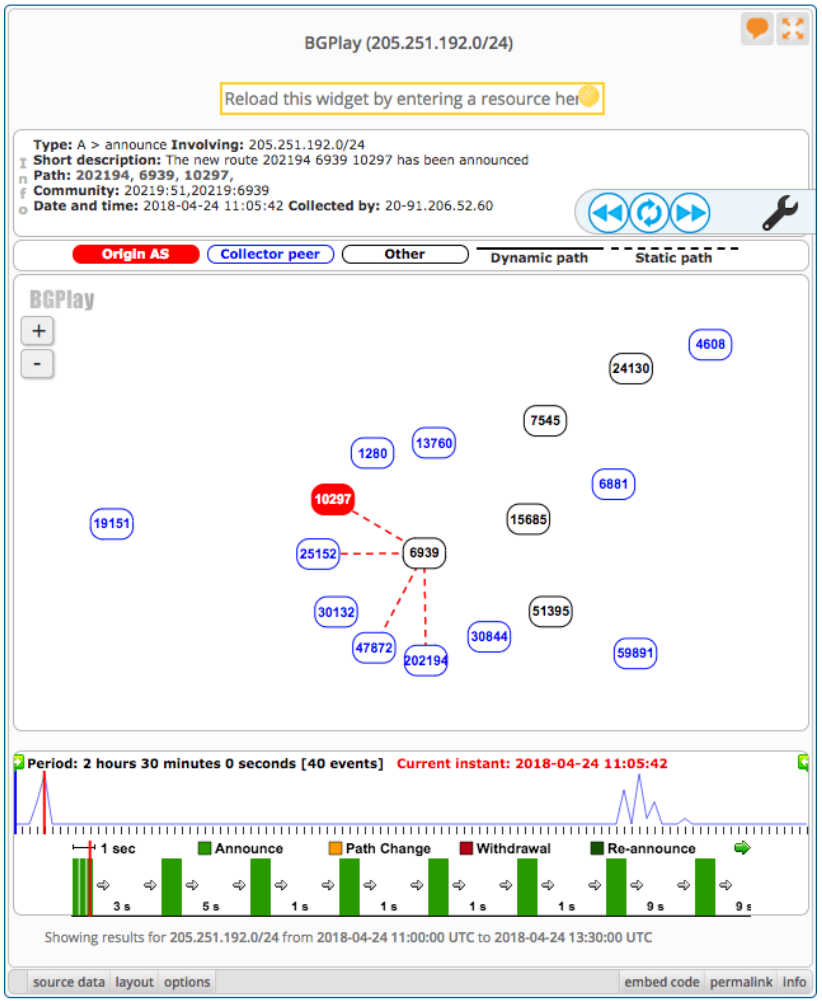
Incident Deep Dive 1: AWS Hijack
Resources

- AWS DNS route announcements:
  - 16509 Originates
    - 205.251.192.0/23
    - 205.251.194.0/23
    - 205.251.196.0/23
    - 205.251.198.0/23
  - AS10297 (eNET, a hosting provider in Ohio), originates more specifics:
    - 205.251.192.0/24
    - 205.251.193.0/24
    - 205.251.195.0/24
    - …

Incident Deep Dive 1: AWS Hijack

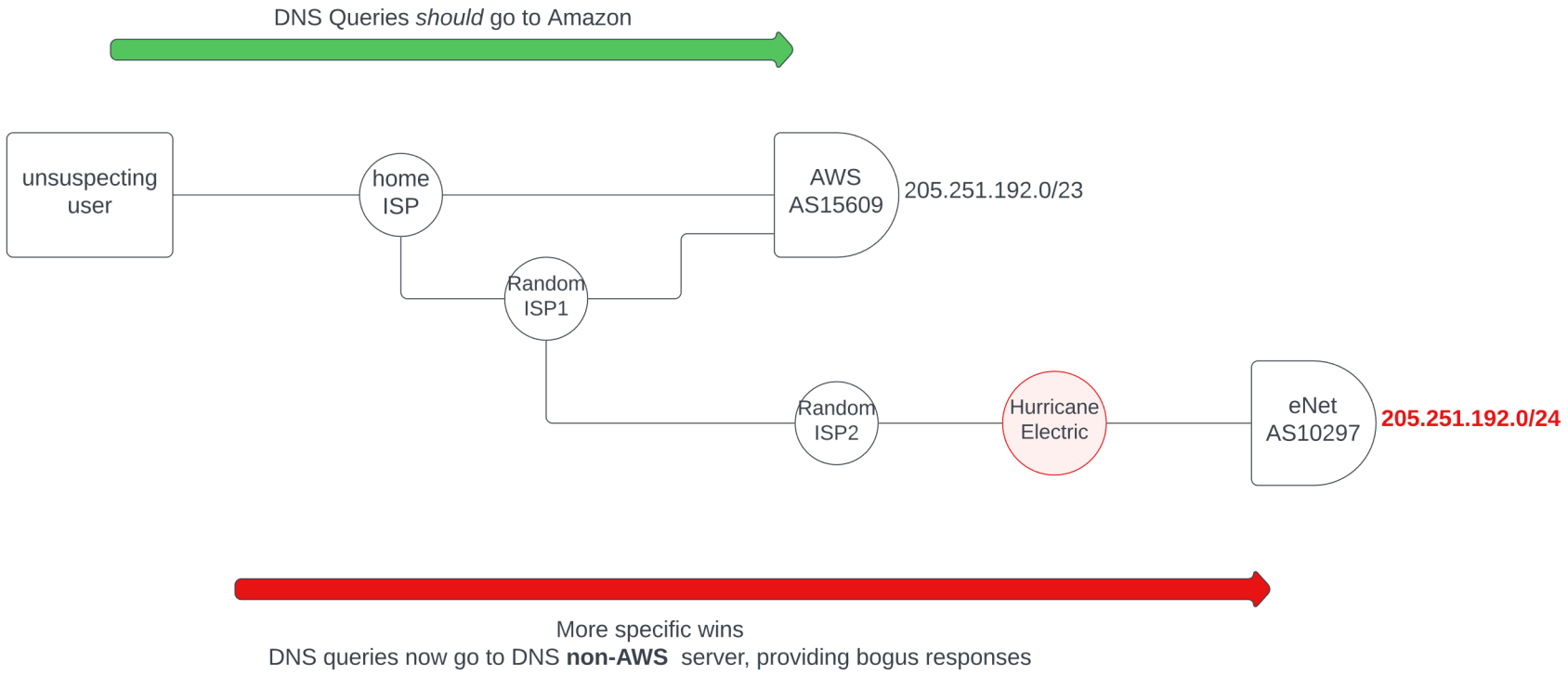
BGP activity

- Bogus announcement accepted by
  - Hurricane Electric (AS6939)
  - 1&1 Internet SE (AS8560)
  - Shaw Communications Inc. (AS6327)
- Not accepted by route server (MLPE) at Equinix-Ashburn



Incident Deep Dive 1: AWS Hijack

DNS relies on BGP!



Incident Deep Dive 1: AWS Hijack

Users misdirected

Incident Deep Dive 1: AWS Hijack
Things That Could Have Helped

- Route filtering (IRR or RPKI-based ROV)
  - Bogus BGP announcement would not have propagated
- DNSSec
  - Bogus records would have rejected bogus records
- HTTP Strict Transport Security (HSTS)
  - Browsers won't accept self-signed certificates (yes, the swindled users were warned, but clicked through)

Other Incidents

- KLAYSwap
  - Also, a crypto-theft event.
  - More sophisticated-
    - Hijack a prefix contain servers hosting Javascript loaded into the main website
    - Certificate was valid (DCV implicitly trusts the infrastructure!)
    - Origin AS was correct (sort of)
- Rostelecom
  - Traffic for Apple Engineering routed through Russia

Effects

- Malicious Activity including theft
- Surveillance
- Reduced performance and availability of the infrastructure
- Loss of Trust in the infrastructure
- Defensive Deaggregation
  - AWS is now announcing /24s instead of /23s
  - Tragedy of the Commons
  - If everyone defensively deaggregated to the commonly accepted longest mask:
    - Additional IPv4 entries*
      - 15,595,508
    - Additional IPv6 entries*
      - 15,467,624,156

* These numbers overstate the situation, especially for v6…there is a /16 in the table, that along accounts for 4.29 billion entries; unlikely that *all* /48s are needed

- MANRS For Network Operators

MANRS Actions – Network Operators Programme

There are four actions for Network Operators

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 global 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 on a global scale

Publish your routing data, so others can validate

Registering number resources in an IRR and/or

creating ROAs for them

The Actions in Operation – *Filtering* (Mandatory)

- Description
  - Network operator must implement a system whereby they only announce to adjacent networks the AS numbers and IP prefixes they or their customers are legitimately authorised to originate.
  - Network operator much check whether the announcements of their customers are correct; specifically, that each customer legitimately holds the AS numbers and IP address space they announce.
  - Possible Implementation mechanism
    - Import/Export prefix filters on BGP sessions
    - AS path filter

The Actions in Operation – *Communication & Coordination* (Mandatory)

- Description

  Network operator must ensure that up-to-date contact information is entered and maintained in the appropriate RIR (or NIR) database and/or in PeeringDB. It is strongly recommended that contact information is made publicly available, but at a minimum must be available to other network operators registered with PeeringDB.

- Possible Implementation mechanism
  - Should be pretty obvious!
  - ARIN already bugs us yearly. Just validate and keep your POCs up to date.
  - Use PeeringDB? Keep that up to date as well (including max prefixes!!)←this is a personal gripe

The Actions in Operation – *Global Validation* (Mandatory)

- **Description**

  Network operators must publicly document their intended routing announcements in the appropriate RIR routing registry, RADB or an RADB-mirrored IRR. This includes ASNs and IP prefixes originating on their own networks, as well as the networks for which they provide transit services.

  A network operator may alternatively implement Action 4: Facilitate routing information on a global scale RPKI in lieu of a publicly documented routing policy.

- **Possible Implementation mechanism**
  - IRR
  - RPKI ROAs (but this isn't enough, despite the term "*in lieu*"
- Lots of discussion around this Action

The Actions in Operation – *Anti-Spoofing* (Recommended)

- **Description**

  A network operator should implement a system that enables source address validation for their own infrastructure and end users, and for any Single-Homed Stub Customer Networks. This should include anti-spoofing filtering to prevent packets with an incorrect source IP address from entering or leaving the network.

  A network operator must test whether their network is able to send packets with forged source IP addresses using the CAIDA Spoofer Software. This is to alert the network operator as to whether their network might be used to originate Distributed Denial-of-Service (DDos) attacks, whilst generating publicly accessible information allowing that network to be checked by others.

- Recommended because external validation/measurement is hard

- MANRS For Network Operators

A New Program for the Global Research & Education Community

WHY?

- The challenges arise when some REN's try to comply with the "Filtering" and "Global Validation" actions.

- Massive mutual backup and multihoming (Makes IRR / record keeping difficult)

- Example:
  - AARnet provided temporary backup to a Chinese network while awaiting permeant facilities.
  - This was a short notice / short term event. What's the IRR-propagation timeline?

A New Program for the Global Research & Education Community

WHY?

- There are currently 120 research and education networks in the world today, with over 25,000 universities behind these networks.

- Address space delegation makes ROA generation difficult
- Legacy Address space (yes, we're still talking about this, but the good news is that it's getting better)

Goals of a New Program?

Proactively encourage all research and education networks to reach MANRS compliance (both Internet Facing and R&E Network facing)

Contribute towards improved techniques and tools to support this goal

Publicize MANRS globally and encourage universal participation

Other Areas of Investigation

The goal of the program is to bring R&Es into the MANRS community be acknowledging their uniqueness, not just relax requirements.

R&E Networks should continue to be network *leaders*

Generalized TTL Security Mechanism (GTSM), RFC 5802

Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages, RFC 9234

Extended BGP Administrative Shutdown Communication, RFC 9003

The TCP Authentication Option (TCP-AO), RFC 5925

Advertise and use Max prefix on eBGP sessions

Participation in shared troubleshooting and research data collection programs (eg, NLNOGRing, RIPE Atlas/Anchor, PerfSONAR, RouteViews)

ASPA (Autonomous System Provider Authorisation), draft RFC

Enhanced uRPF, RFC 8704

Have ideas or comments?

agallo@gwu.edu