APNIC reverse-DNS service outage report: May 2018

ggm@apnic.net

arth@apnic.net

What happened:

- We lost DNSSEC for **`121.in-addr.arpa`**

  Secure64 DNSSEC signer on nx-signer has an unknown bug that caused 121.in-addr.arpa to be signed by previous ZSK, that was no longer present in the DNSKEY resource record.

  This caused DNSSEC validation failure for 121.in-addr.arpa when the zone was republished.

- Timeline
  - 05-05-2018 03:00 – nx-signer completed ZSK rollover for all zones
    - including `121.in-addr.arpa` zone.
  - 08-05-2018 10:30 – GGM raised NOC ticket about DNSSEC validation issue.
  - 08-05-2018 11:40 – Incremented zone serial of `121.in-addr.arpa` on master.
  - 08-05-2018 11:56 – `121.in-addr.arpa` validation test from dnsviz.net returns OK.
- Root Cause/s
  - Unknown bug in the signer that caused `121.in-addr.arpa` to be signed by ZSK that was not in the DNSKEY resource record.

What didn’t happen

- We didn’t self-detect
  - This was found due to community concern in the JP operations community
  - 3 day 9 hour outage does not meet acceptable service levels

- Why didn’t we detect?
  - APNIC monitoring systems were in transition to puppet v5 and had been accidentally left disabled for Secure64 signing checks
- Informal ticketing
  - GGM raised internal NOC ticket from private request in JP community
  - We need better formal reporting lines for these problems
    - This is an NRO wide issue: we need to discuss inter-RIR and inter-NIR NOC 24/7

Remediation

- Corrective and Preventative Measures
  - Apply recent secure64 software update on nx-signer and ia-signer
  - Run multiple DNSSEC monitoring to capture different failure types.
    - Validation using Bind dig & LDNS drill tool has been installed on 6 DNS recursive servers.
  - TXT resource record TTL for all signed zones were reduced to 10min for validation to get non cache data every 15-minute run.
  - Add monitoring, to compare DNSKEY used for signing against DS record in the parent zone.
  - Runbook for operations duty cycle revised to emphasize checks
- NRO Engineering Coordination Group (ECG) is discussing updated contact information and NOC processes.

Community reporting

- We publish service outages at
  - https://www.apnic.net/about-apnic/service-updates/
- This outage report available as
  - https://www.apnic.net/about-apnic/service-updates/service-announcement-8-may-2018/
- Subsequent DNS service issues, remediation work also noted here
  - https://www.apnic.net/about-apnic/service-updates/service-announcement-04-june-2018/
  - https://www.apnic.net/about-apnic/service-updates/service-announcement-07-june-2018/
  - https://www.apnic.net/about-apnic/service-updates/service-announcement-9-august-2018/
  - https://www.apnic.net/about-apnic/service-updates/service-announcement-28-august-2018/