

DNSSEC INCIDENT .NA



2022-10-04 (v1.18)

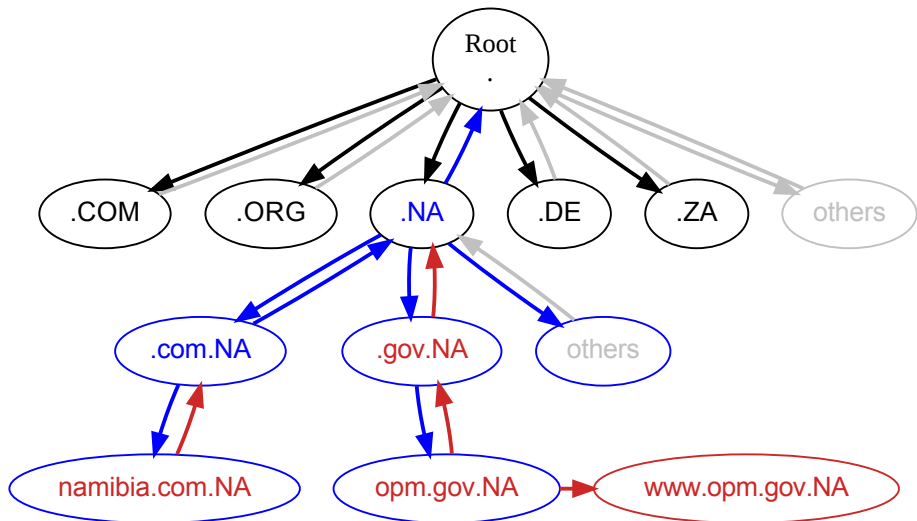
Dr EW Lisse

2023-03-13

Namibian Network Information Center (Pty) Ltd

INTRODUCTION

DOMAIN NAME SYSTEM



BACKGROUND

- .NA Managed Since 1991 (!)
 - Two partial outages previously
 - A few hours each
- Registration Portal
 - CoCCA
- Massively Anycasted
- .NA DNSSEC Signed Since 2009 (!)
 - Previously inline on Hidden Master
 - Since 2020 signed by PCH
 - Hardware
 - Trusted
 - Algorithm 5



TIMELINE

GENERAL REMARKS

- All times are in local time
 - CAT (2 hours past UTC)
- 08:15 CAT (06:15 UTC)
 - Lookup of .NA names failed (email)
- Throughout the Day
 - We Received Numerous Calls
 - Registrars
 - Banks
 - IT Companies
 - We Engaged With
 - Large Registrars
 - Government
 - CERT
- Timestamps



HOUSTON, WE HAVE HAD A PROBLEM!

- 08:17 First Registrar Contacted Us
- 08:25 Web Access to Register Portal Failed
- 08:26 slogin to Register Portal Failed
- 08:27 slogin to portal IP Address succeeded
- 08:30 Name Servers Did Not Resolve
 - .NA Domain Names

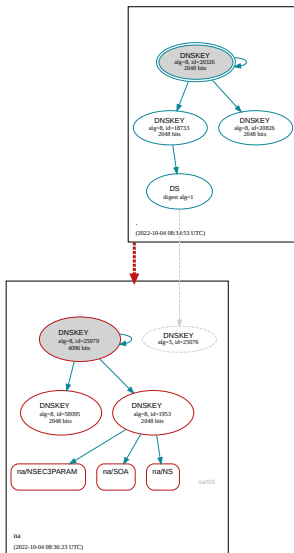


DNSVIZ TO THE RESCUE

- We did **NOT** try
 - `dig @na-ns.anycast.pch.net na ns`
 - `dig @na-ns.anycast.pch.net na ns +cd`
- **BUT** went straight to
 - <https://dnsviz.net>



DNSVIZ



SPEED DIAL

- 08:58 We Phoned PCH
- 09:01 We Raised an Email Ticket with PCH NOC
- 09:10 PCH Phoned Us Back
 - Setting Up Video Bridge
 - Very short URL
 - Lining Up Engineers
- 09:22 We accessed the Bridge
 - PCH Confirmed the Issue
 - Missing DS Record after Algo roll from 5 to 8
 - We Looked at the Options



DECISION TIME

- 09:37 Options Identified
 1. Unsign
 - Would work, but Counterproductive
 - Root zone reload required
 2. Roll-Back to Algo 5
 - Never been done
 - No root zone reload required
 3. Go through with Roll to Algo 8
 - Root zone reload required
- 09:38 PCH emailed Algo 8 DS Record (Option 3)



WAKE UP IANA FUNCTION OPERATOR

- 09:44 We emailed PTI (00:44 PST)
- 09:45 We Phoned PTI's After Hour Service
 - Accented English
 - Communicated Well
- 10:32 PTI's Technical Director Called Back
- 10:39 We Uploaded the New DS Record to RZM
- 10:40 We phoned PTI TD
- 10:44 Automated Response by RZM Received
 - Technical Check Failed
- 10:47 Cell Phone Credit Ran Out
 - PTI TD phoned us back immediately



WORKING THE PROBLEM(S)

- 11:23 PCH Engaged With PTI
 - Telephone
 - Email
- 11:46 PTI called PCH
 - Confirmed correct DS Record
 - Manual Override
 - Forwarded to Verisign
- 11:50 Approval Link Received From PTI
 - Email
 - Technical Contact
- 12:19 We Approved from **BOTH** Contacts



THE EAGLE HAS LANDED!

- 13:37 H.root-servers.net Received Zone
- 13:41 We Noticed Beginning Resolution
- 13:42 We Received Email Confirmation From PTI
- 13:46 PTI Engineering Phoned PCH
- 13:49 PTI TD Emailed Confirmation



CLEAN UP

- 16:07 PTI Engineering Phoned PCH
 - Requested removal of old DS Record
- 16:17 PCH Emailed Us
 - Requested removal of old DS Record via RZM
 - Done immediately
- 16:19 PTI RZM Acknowledged Request
 - We approved immediately
- 16:45 Old DS Record Removed



AFTERMATH

- Media
 - Contacted us the following day
 - We only engaged with one newspaper
- Banks
 - Very satisfied with the outcome
 - and the engagement
- Registrars
 - *No Drama*
- Government
 - Initially concerned about attack (on infrastructure)
 - Very receptive of (early) engagement
 - *technical glitch*



LESSONS LEARNED

DON'T PANIC!

- *Work the Problem!*
 - It's only technology
- Work the Checklist
 - If you have one
 - You really **should** (have one)
- *Don't Make Things Worse by Guessing!*
 - It's not Rocket Science
- DNSViz is Your Friend
 - Off line tool?



SPEED DIAL

- PTI
 - **After Hours**
 - +1 (310) 306-6308
 - **During Hours**
 - +1 (424) 254-5300
- Join TLD-OPS
 - <https://ccnso.icann.org/en/resources/tld-ops-secure-communication.htm>

There is Always Someone on the Other End of the Line (M Lawrie, 1994)



CHECKLIST

- Write a *Handbook*
 - Document Processes
 - Does not have to be ISO
 - Update **Frequently**
- Practice Scenarios
 - Loss of KSK
 - Failed Roll
 - Loss of Name Server(s)
 - Interaction with IFO
 - RZM
 - Staff
 - Others



PRACTICAL TIPS

- Separate (Email) Domains for
 - Admin Contact
 - Technical Contact
- Communicate
 - CERT (if any)
 - Registrars
 - Media
- Have your Provider on Speed Dial
 - Have them have you on Speed Dial
- Have Sufficient Credit on the Cell Phone
 - Consider Landline



QUESTIONS?

THANK YOU!

- Packet Clearing House
 - Director
 - Engineers
- Public Technical Identifiers (IFO)
 - Technical Director
 - Engineers



Questions?