.ke DNSSec Update

Toilem Poriot Godwin

.ke DNSsec update

- Update on what .ke registry experienced
- 30th April 2015-- Longest mornings I have ever had.
- Day started as usual but takes a turn at 9:30am
- Great day turns to a "Dark Day"

What happened

- Received call from registrar his .ke domains are not accessible
- There are challenges where most registrars have not mastered how to troubleshot DNS
- Thought its one of the situations a registrar has DNS misconfiguration on their name server
- All domains in my LAN/DNS were accessible

When DNSsec Goes Wrong

- All domains in my LAN/DNS were accessible
- Government Websites/Domains were accessible
- Later I noticed most domains whose nameservers refreshed cache after 5 hour were inaccessible
- Question of DNSSec and Inaccessibility of domains later arose---Why these domains were accessible at all-- thought all request to a domains will be rejected if keys/signatures didn't match

Troubleshooting

- Started doing DNS troubleshooting on my LAN
- Started troubleshooting DNS on registrars LAN/ Server
- Thought I should check on DNSSec since all configs were ok.
- Alas to my surprise my signatures had expired

Troubleshooting cont..

- My signatures were set to expire a month after the day the signatures were revoked
- I had set DNSSec-auto-maintain to on--Big mistake
- DNSSec Auto-mantain on is the default setting to some bind versions
- Saw my keys as bogus.

Resolve the Problem

- Panic... panic... Panic... never experienced a DNSsec breakdown before.
- Contacted IANA to remove the DS records from the root---- another big mistake--IANA acts on DNS changes within 24 hours and if everything checks out your request may be completed in 72 hours
- .ke domains were offline and our primary contacts were .ke we could not receive IANA's confirmations. This took me around 30 minutes to understand since I could receive emails from other domains.
- Return to the option that I should have used first, find my keys That i used to generate the signatures and resign the zone.

Resolve Problem cont……

- Got the keys but for some reason the seemed corrupt.
- Found one key with same key tags on DS and resigned the domain
- Zone came up but had issues with bogus Serial records.
- With this bogus record .ke domains were still accessible--begs the question how DNSSec checks records and blocks queries again????

Preventing future DNSSec Failures

- Set DNSSec Automaitain to off
- Detailed DNSSec Monitoring
- Rigorous test on DNS Server for any bugs report or find a work around

Lessons Learned

- If DNSSec fails in a registry environment try restoring your keys than removing DS records
- Communication to
- Practice on all possible DNSSec Failures.
- Check on DNSSec maintain, Compare pros and cons on setting Auto-maintain on or off

END.....

Thank You