DNSSEC Deployment for Network Operators

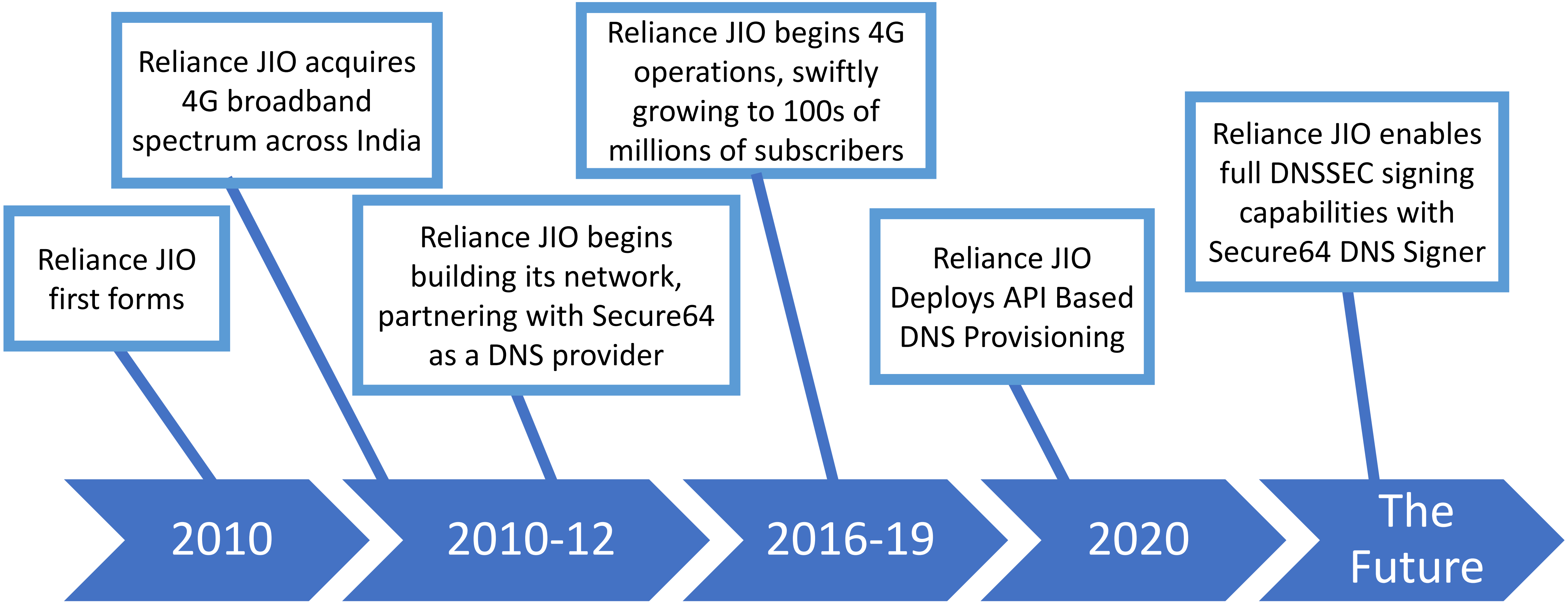
Presented by Molay Ghosh

Reliance Jio Infocomm Ltd

Agenda

- Reliance Jio throughout the years
- What is DNSSEC?
- Hijacking the DNS
- DNS Hierarchy in JIO
- Cost of DNS Hijacking
- Reliance Jio DNS Deployment
- DNSSEC Queries Validation Stats
- DNSSEC Deployment
- Impact on DNS KPI
- Issues seen in DNSSEC implementation in Jio Network
- APNIC Reference data for JIO AS 55836

Reliance JIO Through the Years



2010

Reliance JIO first forms

Reliance JIO acquires 4G broadband spectrum across India

2010-12

Reliance JIO begins building its network, partnering with Secure64 as a DNS provider

2016-19

Reliance JIO begins 4G operations, swiftly growing to 100s of millions of subscribers

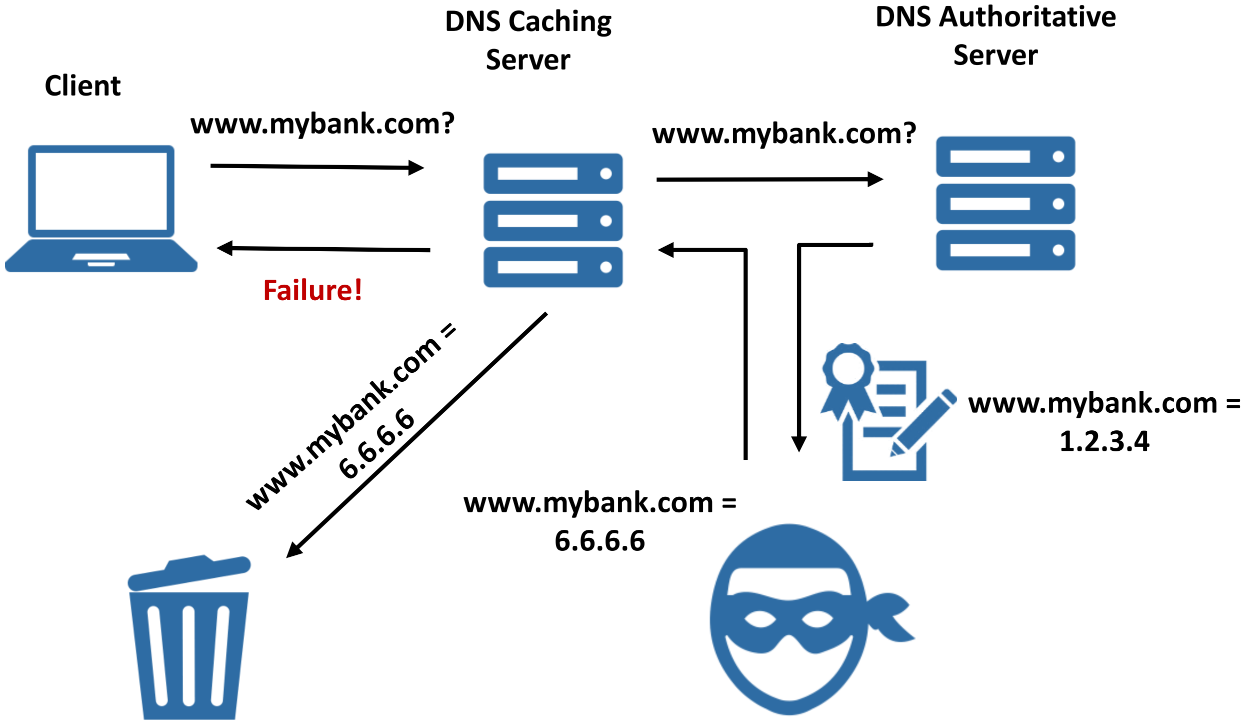
2020

Reliance JIO Deploys API Based DNS Provisioning

The Future

Reliance JIO enables full DNSSEC signing capabilities with Secure64 DNS Signer

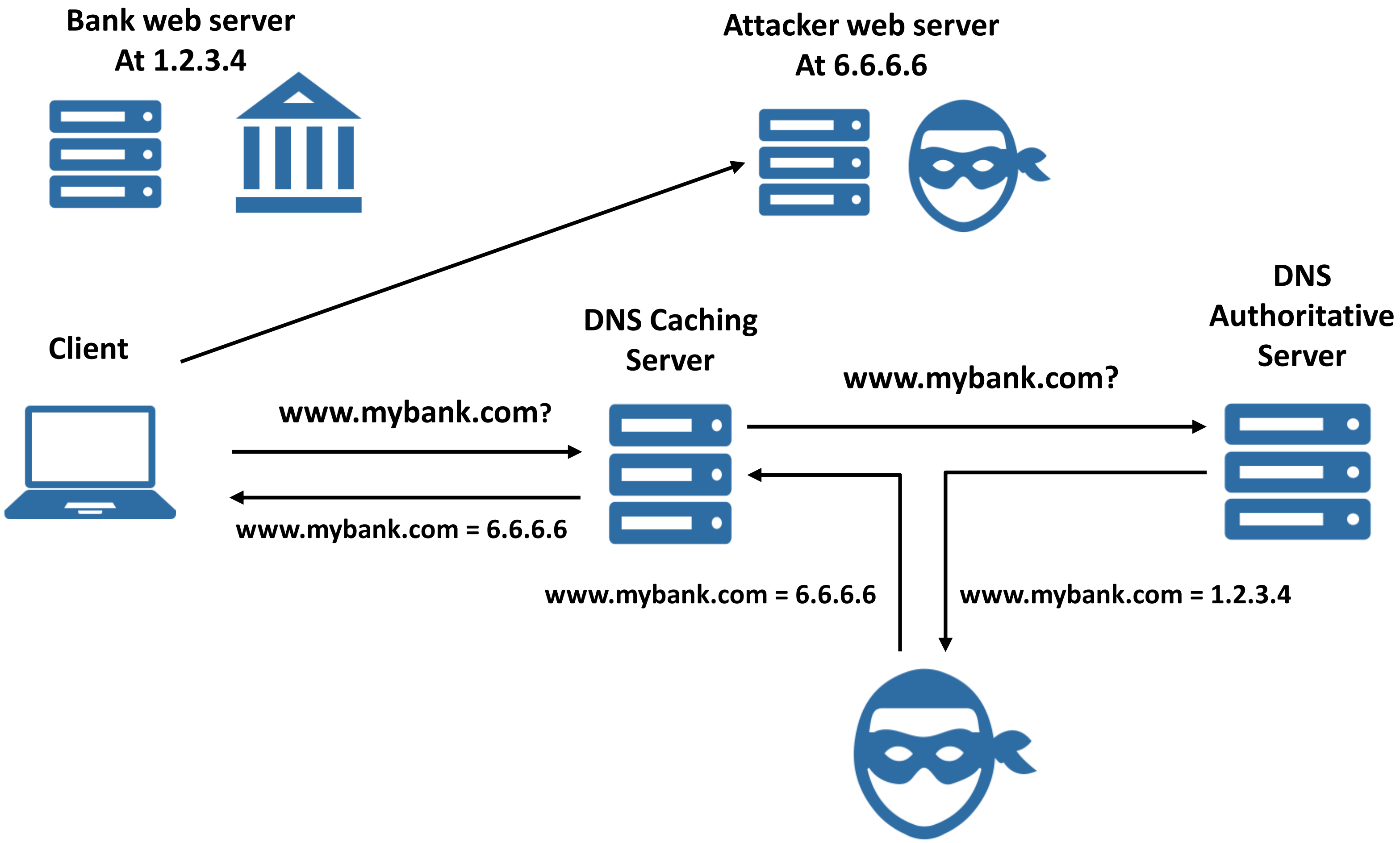
What Is DNSSEC?



- Authoritative Server
- Digitally signs answer
- Adds signature to response

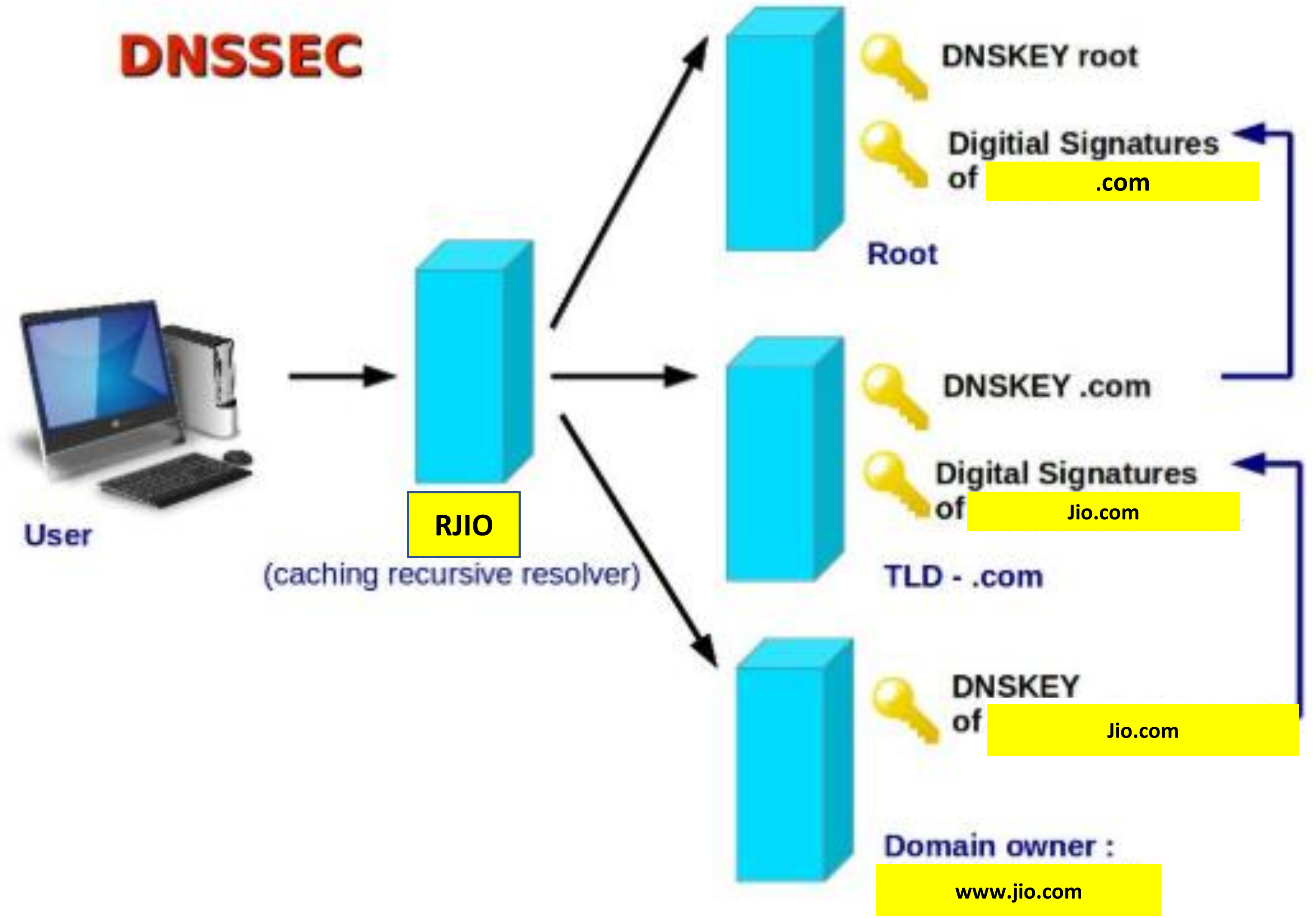
- Caching Server
- Verifies digital signature
- Does not transmit invalid responses to clients

Hijacking the DNS



All Rights Reserved Reliance Jio-CONFIDENTIAL

DNS Hierarchy in Jio



The Cost Of DNS Hijacking

Brand Damage

Your name on the front-page news

Downtime

Web servers may be unreachable

Loss of revenue for e-business

Liability

Hijacked organization may be liable for damage to consumers

Funds Theft

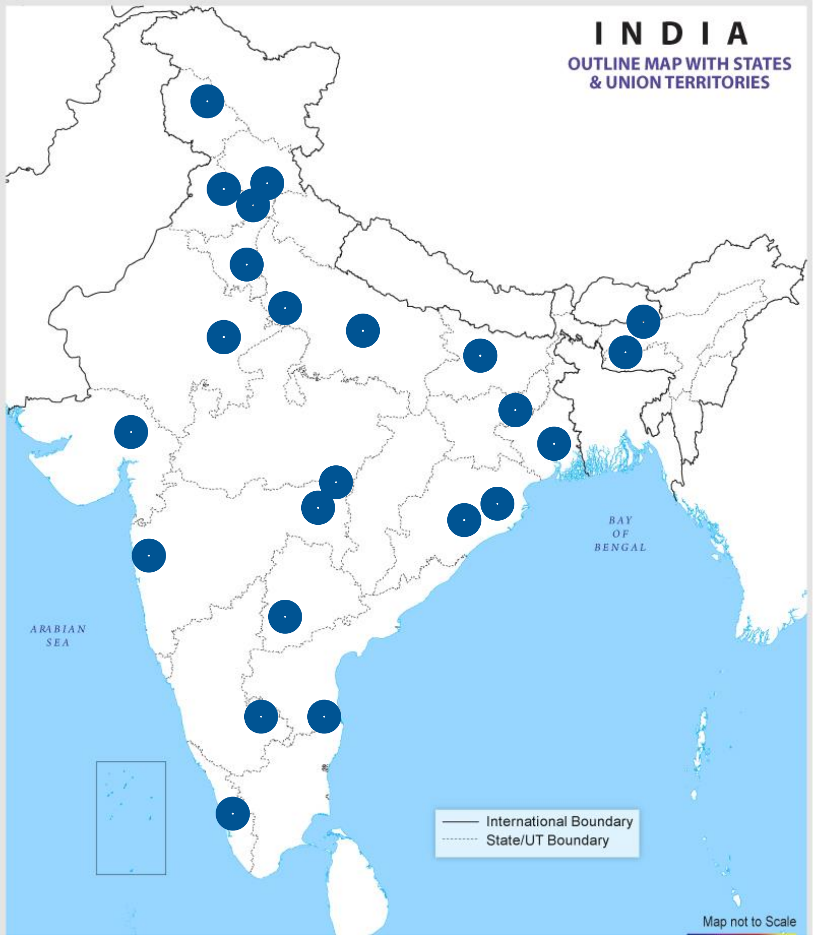
Email compromise can lead to loss of company funds through spear phishing

IP Theft

Email compromise can leak confidential info

Reliance JIO DNS Deployment

SECURE 64®



370 Mn subscribers across over 30 sites

(6) Authority servers

(158) Cache servers

(2) Manager servers

(2) Signer servers

Peak QPS per Server

0.35 Mn

Total Peak QPS

15.9 Mn

DNSSEC Queries Validation

% of Queries Validated

94.56 %

% of Partial Validation

4.67%

% of Failure Validation

1.8%

DNSSEC Configuration

Configuring the Secure64 DNS resolvers to support DNSSEC was as simple as adding two lines to the configuration file, for both SourceT and x86 servers

[Source : https://stats.labs.apnic.net/dnssec/AS55836](https://stats.labs.apnic.net/dnssec/AS55836)

DNSSEC Deployment

- JIO have deployed 158 Cache DNS Servers configured to accept DNSSEC, the next step is to implement Secure64’s DNS Signer for Authoritative Zones.

- DNS Signer will enable centralized, scalable signing capabilities for our caching servers, further protecting our subscribers from threats like DNS hijacking for Jio Owned domains.

- RJIO has enabled DNSSEC in all Cache (Resolver) DNS Servers with New KSK Keys (. IN DS 20326 8 2E06D44B80B8F1D39A95C0B0D7C65D08458E880409BBC683457 104237C7F8EC8D)

Impact on DNS KPI

Sr. No.	KPI	Impact
1	Query Per Second (QPS)	No adverse affect
2	Cache miss latency	No adverse affect
3	CPU Usage	No adverse affect
4	Memory Usage	increased by 2%
5	Cache hit ratio	No adverse affect

Issues in implementation DNSSEC in JIO

- Post deployment, Subscriber were not able to resolve below websites , after troubleshooting found that due to enabled DNSSEC on resolver, it was not able resolve these websites.

- www.anedapps.com
- www.njoycabs.com

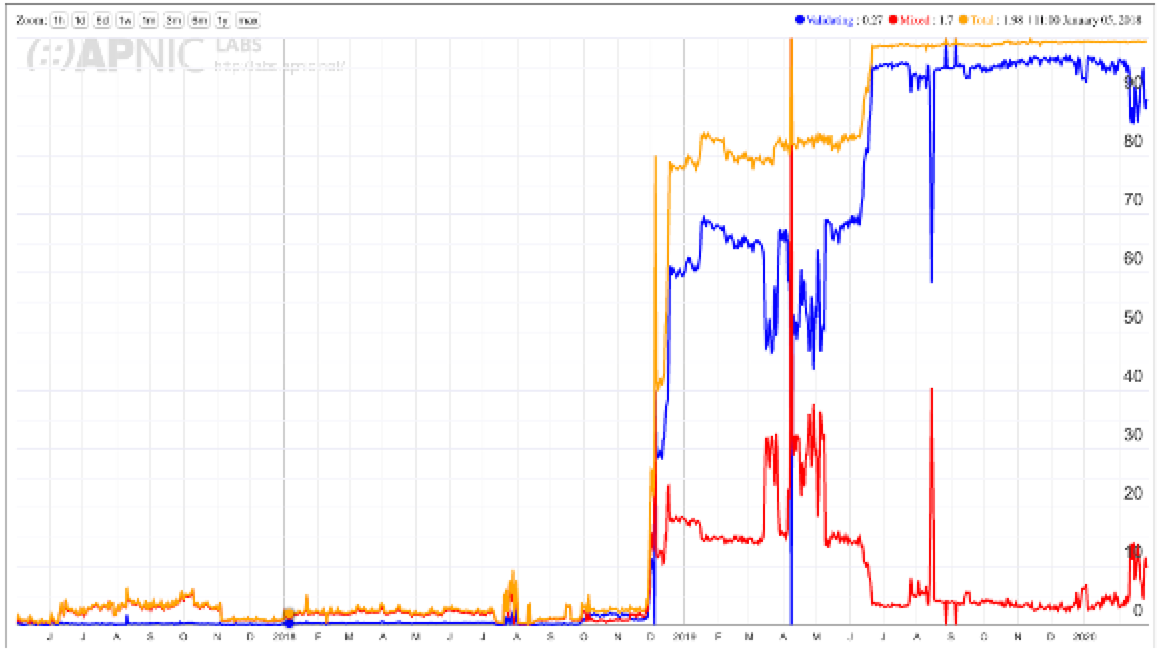
- Why it was not working ?

- Resolver was doing DNSSEC (RRSIG,DNSKEY) query but getting no response/invalid response, hence for resolver it was not secured domain and same was not resolving for the subscriber.

- RJIO has communicated same to respective authoritative name server owner , after corrective measure , now both websites are working fine.

APNIC Reference Data for AS 55836 JIO

AS55836: RELIANCEJIO-IN Reliance Jio Infocomm Limited, India (IN)



In this case, 2019. In India, the mobile provider Reliance Jio, who is clearly India's largest ISP, has made this decision to enable DNSSEC validation in late 2018, completing the work by mid-2019 .

https://stats.labs.apnic.net/dnssec/AS55836

https://blog.apnic.net/2020/03/02/dnssec-validation-revisited/

Thank You