.ZA COMMERCIAL SECOND LEVEL DOMAINS (SLDs)

CO.ZA | ORG.ZA | NET.ZA | WEB.ZA

INCIDENT REVIEW

March 2025 DNS Outage and Degradation

Lessons Learned and Operational Improvements

Original Report Issued: 20 May 2025

Public Release: July 2026

CO.ZA 30 YEARS

POWERED BY ZARC

**** Public Release Notice ****

This document constitutes the public-release edition of the final incident report, originally issued on 20 May 2025. Unless otherwise indicated, the contents reflect the information available at the time the original report was finalised. A Post-Incident Update summarising subsequent operational improvements and additional findings has been included at the end of this document.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved.

Foreword to Public Release (July 2026)

This report was originally finalised on 20 May 2025 following the DNS outage and degradation experienced in March 2025, and was prepared for limited distribution to key stakeholders.

At the time of its completion, the report was provided to the ZA Domain Name Authority (ZADNA) and the relevant public authorities. Owing to the ongoing technical review and associated security-related investigations being undertaken at the time, wider publication of the report was deferred pending the conclusion of those processes.

Since the incident, ZARC has continued to analyse operational telemetry, implement infrastructure and operational improvements, and incorporate the lessons learned into the ongoing evolution of its DNS architecture, operational procedures and resilience planning. This work has strengthened both the robustness of the Shared Registry System (SRS) and the registry's preparedness for future operational events.

Following requests from accredited registrars and members of the Internet Service Providers' Association (ISPA) Domain Name Working Group, and with the agreement of the ZA Domain Name Authority, this report is now being released in the interests of transparency, industry collaboration and strengthening the resilience of South Africa's DNS infrastructure.

This document should therefore be read as a historical record of the incident based on the information available when the original report was finalised in May 2025. Subsequent operational developments, additional technical analysis and the implementation of further mitigation measures are summarised in the Post-Incident Update included at the end of this document.

ZARC believes that openly sharing operational experience, lessons learned and continuous improvements contributes to a stronger, more resilient Internet ecosystem. It is in that spirit that this Incident Review is published.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Table of Contents

Foreword to Public Release (July 2026) **2**
Basic Information **4**
Incident Description & Summary **4**
Equipment or Systems Affected **5**
Impact Assessment 6
Root Cause Analysis **6**
Contributing Technical Triggers 6
Compounding Factors 7
Underlying Factors 7
Supporting Evidence 8
Actions Taken **8**
Resolution and Preventive Measures **8**
Final Resolution 8
Lessons Learned 9
Further Recommendations for Prevention & Mitigation 10
Follow-Up Actions 11
Report Approval & Submission **11**
Schedule 1 - Evidence **12**
Section A: DNS Query and Traffic Volume Charts 12
Section B: Packet Capture showing NXDOMAIN queries 16
Section C: System Resource Utilisation Charts 17
Post-Incident Update (July 2026) **18**

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Basic Information

- **Incident Period**: 6-14 March 2025
- **Incident Report Number**: ZRS-7331 (JIRA)
- **Incident Description:** DNS Degradation and Outage
- **Incident Type:** Service Disruption & Outage, Security Event
- **Location:** Global
- **Resources Involved:** ZARC DevOps and Registry Operations Teams

Incident Description & Summary

Between 6 and 13 March 2025, the ZARC registry experienced a significant operational incident affecting portions of its authoritative Domain Name System (DNS) services. The incident arose from the interaction between planned DNSSEC changes and an abnormal increase in DNS query traffic

As part of an ongoing programme to strengthen and improve cryptographic security and resilience, ZARC initiated the rollout of new Hardware Security Modules (HSMs) in February 2025. On 6 March 2025, the registry implemented a *2048-bit RSA* Zone Signing Key (ZSK), in line with security recommendations from ICANN's KINDNS initiative[1].

While the introduction of the larger ZSK did increase DNS response sizes, particularly for NSEC3-signed zones such as those employed by ZARC in its Shared Registry System (SRS), this alone would not have destabilised DNS operations under normal conditions. A significant contributing factor was a concurrent, abnormal increase in NXDOMAIN query traffic exhibiting characteristics consistent with an NXDOMAIN Flood. This abnormal query behaviour rapidly inflated total DNS traffic volume and placed disproportionate load on unicast nameservers.

The result was a substantial increase in overall DNS traffic, particularly affecting unicast nameservers, some of which began to exhibit signs of strain, including delayed zone propagation, intermittent flapping (the rapid and repeated oscillation of a network device, link, or route between operational/failed states), and inconsistent serial synchronisation. While the Anycast infrastructure performed reliably throughout the incident, absorbing and distributing traffic across its global footprint as designed, the unicast servers, including third-party-operated infrastructure, were under significant pressure.

To mitigate the situation, DDoS protection measures were implemented, including rate limiting and query filtering. These were partially successful in reducing load, but on 12 March, a sharp spike in malicious traffic further overwhelmed several unicast servers. Logs and packet captures identified traffic patterns consistent with an NXDOMAIN Flood,

[1] As part of the KINDNS onboarding process for the .ZA SLDs, ZARC engineers were directed to use the https://zonemaster.net/ online diagnostic tool for the SLDs and to address any subsequent errors. This tool issued a key size warning, indicating that the recommended key size is 2048-bit.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

characterised by a high volume of spoofed (a deliberate falsification of network communication data to impersonate a trusted source) and non-existent record queries, largely targeting DNSSEC-enabled zones via both UDP and TCP.

By 13 March, the engineering team determined that the combination of large responses from the 2048-bit ZSK and sustained abnormal traffic patterns could not be mitigated effectively without altering the signing parameters. As a result, an emergency ZSK rollover was executed, replacing the 2048-bit key with a smaller 1024-bit ZSK to reduce reply packet sizes and return to predominantly UDP-based resolution patterns.

While the rollover was completed successfully, it is acknowledged that this emergency action temporarily resulted in a partial outage of DNS resolution for some relying parties. Specifically, DNS resolvers that had cached the previous key or had not yet updated to the new key, particularly those that are DNSSEC-validating, may have rejected DNS responses during the period when key information was out of sync. This would have resulted in DNS lookup failures for some users, depending on the resolver's cache state and DNSSEC awareness. The impact of this issue was limited in duration and, based on resolver TTLs (Time-To-Live) and observed traffic normalisation, is estimated to have lasted no more than two hours, with a progressive decline in severity as updated DNSKEY records propagated through the caching resolver ecosystem.

This incident highlights the evolving threat landscape facing DNS infrastructure, particularly how adversarial conditions such as targeted DDoS attacks, in the form of an NXDOMAIN Flood, can exploit or amplify the effects of otherwise routine infrastructure changes. The incident reinforces the need for enhanced real-time monitoring, staged cryptographic rollouts, and DNS service architectures that can adapt to aggressive query amplification and abuse patterns. Future enhancements will prioritise phased deployment mechanisms, early detection of anomalous resolver behaviour, and greater resilience under cryptographically intensive conditions.

Equipment or Systems Affected

The incident primarily affected the registry's authoritative secondary nameserver infrastructure, which plays a critical role in the stability and availability of the registry's DNS services. During sustained periods of abnormal query volumes, including elevated NXDOMAIN query traffic and increased DNS response sizes associated with the concurrent DNSSEC key change, portions of the unicast authoritative nameserver infrastructure experienced performance degradation, including intermittent service instability ("service flapping").

In addition to the nameserver infrastructure, the network infrastructure responsible for managing and filtering inbound DNS traffic came under significant load during the peak of the incident (12 and 13 March). This placed significant additional demand on network processing resources and associated monitoring systems during the peak of the incident. Overall, different components of the authoritative DNS platform experienced varying levels of operational impact, reflecting the differing roles and resilience characteristics of the underlying infrastructure.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Impact Assessment

- **Operational Disruption** - While Anycast DNS resolution services remained largely stable during the initial stages of the incident, unicast systems experienced sustained strain due to an anomalous increase in query volume, resource exhaustion, and delayed zone propagation. Notable operational disruption occurred during an emergency ZSK rollover window (13th March), when some external resolvers may have experienced intermittent DNSSEC validation failures, leading to temporary resolution issues.
- **Reputational Harm** - Although the incident was largely contained and public-facing services continued to operate via our robust Anycast infrastructure, the visibility of DNS instability (particularly during the emergency ZSK rollover phase) posed a risk to stakeholder confidence and could affect perceptions of reliability and trust in the registry's operations.

Root Cause Analysis

The incident developed during a sustained period of abnormal NXDOMAIN query traffic exhibiting characteristics consistent with an NXDOMAIN Flood event. The operational impact resulted from the interaction between this abnormal traffic, concurrent DNSSEC infrastructure changes and existing capacity limitations in portions of the authoritative DNS environment. This abnormal and sustained query pattern generated excessive cryptographic and processing load on the registry's authoritative (unicast) name server infrastructure, including DNSSEC-signed zones that employ NSEC3 for authenticated denial-of-existence.

Compounding this attack was a concurrent infrastructure change: the planned rollout of a larger 2048-bit Zone Signing Key (ZSK) for DNSSEC. While cryptographically sound and aligned with best-practice recommendations, the ZSK upgrade increased the size of DNS responses, particularly NXDOMAIN responses, pushing many responses beyond the UDP packet threshold and triggering TCP fallback. This introduced additional system overhead and performance strain.

Contributing Technical Triggers

- NXDOMAIN Amplification under DNSSEC:
    - NXDOMAIN responses, especially in DNSSEC zones that use NSEC3, are computationally expensive and verbose because they require a cryptographic proof of non-existence.
    - These responses were being exploited or, coincidentally, aligned with a concurrent surge in suspicious traffic, including a high volume of queries for non-existent subdomains, amplifying the impact of the change.
- TCP Fallback and Packet Truncation:
    - DNSSEC-signed responses exceeding the practical UDP size limit (1232 bytes) led to frequent packet truncation and TCP fallback. The connection

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

overhead introduced by TCP placed further load on unicast name servers, many of which experienced elevated resource demand during sustained TCP traffic.

Compounding Factors

- Emergency ZSK Rollover Timing: In response to rising system pressure, an emergency ZSK rollback to a smaller 1024-bit key was initiated to reduce response payloads and restore operational stability. However, some DNSSEC-validating resolvers experienced temporary validation mismatches during the transition window, resulting in short-lived resolution failures.

- Network Infrastructure Strain: The increased volume of TCP and fragmented traffic also placed downstream strain on the firewall infrastructure, leading to connection-tracking issues and increased latency in packet inspection.

Underlying Factors

- ZSK Size and Timing: The transition to a 2048-bit Zone Signing Key (ZSK) increased DNSSEC signature size, significantly inflating response payloads, particularly for negative responses such as NXDOMAIN. The key rollover was implemented under operational constraints that limited the extent of production-scale performance validation. As a result, there was limited opportunity to assess potential resolver behaviour, cache propagation timing, and the impact on infrastructure under live conditions.

- NXDOMAIN Flood: During the rollover window, a concurrent, sustained pattern of high-volume DNS queries targeting non-existent CO.ZA domains was observed, with many exhibiting signs of algorithmic generation. This query traffic aligns with the characteristics of an NXDOMAIN flood attack (DNS water torture), where randomised domains are used to evade caching, overload authoritative servers, and exploit the cost of negative DNSSEC responses. The timing and structure of these queries suggest they were automated and consistent with malicious activity.

- DNSSEC Amplification: The SLD zones (particularly CO.ZA) utilise NSEC3 for authenticated denial-of-existence, which, when combined with the larger 2048-bit ZSK, resulted in NXDOMAIN responses that regularly exceeded the recommended UDP size threshold (1232 bytes). This triggered widespread UDP truncation and fallback to TCP, compounding the server's processing and memory overhead. The response amplification effect also increased outbound bandwidth, adding strain on the system's DNSSEC signing, buffering, and session-handling capabilities.

- Unicast Infrastructure Limitations: The targeted unicast secondary name servers experienced resource constraints. Unlike the Anycast nodes, which successfully distributed traffic load, the unicast infrastructure presented opportunities for additional resilience improvements, resulting in localised performance degradation, flapping, and periods of unresponsiveness. This gap in resilience contributed to the observable impact on service at the peak of the incident.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Supporting Evidence

- DNS Query and Traffic Volume Charts from Netnod and Internal Logging Systems (Refer to Schedule 1, Section A)
- Packet capture files showing NXDOMAIN queries (Refer to Schedule 1, Section B)
- System Resource Utilisation during the Peak Incident Window (Refer to Schedule 1, Section C)

Actions Taken

To mitigate the impact of the escalating DNS degradation and restore system stability, the response team executed an emergency rollback to a smaller 1024-bit Zone Signing Key (ZSK) on 13 March. This decision was made in the context of sustained query pressure attributed primarily to a high-volume NXDOMAIN flood event, consistent with a targeted DDoS attack. While the increased response size introduced by the 2048-bit ZSK contributed to resource strain, it was the surge in malicious traffic that rendered the system vulnerable under stress.

The rollback aimed to reduce cryptographic payload sizes, alleviate TCP fallback rates, and restore DNS resolution performance across unicast infrastructure. This change, however, introduced short-term challenges in propagation and validation.

Subsequent analysis suggests that temporary inconsistencies in DNSSEC key propagation were observed during emergency remediation. This likely resulted in intermittent DNS resolution failures for some DNSSEC-validating clients, depending on resolver configurations, key caching, and refresh intervals.

This partial outage is estimated to have lasted up to two hours, during which affected resolvers may have temporarily relied on stale DNSSEC key material. This conclusion is supported by observed TTL expirations, DNS telemetry trends, and corroborating outage reports from impacted networks.

Resolution and Preventive Measures

Final Resolution

- **Network Traffic Mitigation**: To counter continued abnormal query volumes, targeted mitigation actions were implemented. These included:
    - Blocking the network subnets associated with anomalous query activity.
    - Deploying enhanced traffic filtering measures at strategic ingress points.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

- **Emergency Key Rollover**: A new, smaller 1024-bit DNSSEC Zone Signing Key (ZSK) was generated and deployed as part of an emergency rollover procedure, replacing the previously introduced 2048-bit key. The larger key was formally retired from the zone to reduce response sizes and alleviate pressure on TCP fallback.
- **DNSSEC Error Resolution**: Intermittent resolution issues, likely due to key propagation delays and resolver cache inconsistencies, were resolved after the rollback.
- **Nameserver Restoration**: The original authoritative name server was successfully reinstated following a full system restore. Its original IP address was reassigned, and the server underwent a resource upgrade to double its CPU and memory capacity, significantly improving its ability to handle peak loads.
- **NameServer Expansion**: To improve resilience and provide greater geographic and operational redundancy, an additional authoritative name server was deployed into production and integrated into the CO.ZA zone.
- **DNS Software Upgrade**: The authoritative DNS software stack was modernised. This change improves overall query throughput, reduces memory overhead, and enhances the server's ability to withstand DNS-based DDoS attacks.

Lessons Learned

- **DDoS Preparedness and Response:** This incident confirmed the growing sophistication and impact of NXDOMAIN flood-based DDoS attacks targeting DNSSEC-enabled zones. Real-time anomaly detection, faster traffic classification, and upstream mitigation capabilities must be central to operational preparedness. Improving visibility into DNS query patterns, traffic sources, and the evolving characteristics of malicious activity will enable earlier detection, faster response, and greater resilience against future attacks.
- **Emergency Key Rollovers**: The incident highlighted the importance of strictly following established procedures for emergency DNSSEC key rollovers, particularly those outlined in RFC 7583 (DNSSEC Key Rollover Timing Considerations) and the DNS Institute's operational best practices. A structured, pre-tested emergency key management plan, including advance publication, propagation monitoring, and fallback protocols, is essential to avoid service disruption during high-pressure scenarios.
- **Communication with ZADNA**: The event underscored the need to continue strengthening collaboration with ZADNA (ZA Domain Name Authority) to facilitate swift coordination during operational emergencies. Establishing formal escalation pathways and change notification mechanisms will improve agility and transparency during time-sensitive changes.
- **Stakeholder Communication**: Clear, timely, and consistent communication with registrars, ISPs, resolver operators, and other stakeholders is vital during incidents that impact domain resolution. A formalised stakeholder incident communication

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

plan, including predefined messaging templates and escalation contacts, should be adopted and regularly tested.

- **Cryptographic Algorithms**: Using larger RSA-based ZSKs introduced performance and response-size challenges during the incident. This reinforces the value of transitioning to modern cryptographic algorithms such as ECDSA (#13), which offer equivalent security with significantly smaller key sizes and lower computational and network overhead. Algorithm agility must be incorporated into DNSSEC operational planning.

- **National Anycast Network**: The observed impact on unicast infrastructure highlights the need to explore deploying a dedicated national (local) Anycast DNS network to serve queries from South African users more efficiently. Local Anycast nodes can improve performance, limit exposure to global DDoS vectors, and enhance service continuity during high-traffic or attack scenarios.

Further Recommendations for Prevention & Mitigation

- **DDoS-Resilient Infrastructure Scaling and Load Testing:** Enhance the scalability and resilience of authoritative DNS infrastructure to withstand sudden, potentially malicious traffic spikes. Proactive stress testing and simulated DDoS attacks, including NXDOMAIN floods, should be prioritised as a critical component of resilience planning. These exercises validate system resilience and behavioural integrity under realistic adversarial load conditions, with heightened emphasis during high-risk maintenance windows such as DNSSEC key rollovers or infrastructure upgrades.

- **Precision DoS Protection Tuning:** DoS mitigation systems must be finely calibrated to distinguish between legitimate load increases and attack vectors. Adaptive rate limiting, anomaly detection, and auto-escalation mechanisms should be implemented with context-aware thresholds to maintain service availability while deflecting abuse.

- **Advanced Real-Time Telemetry and DDoS Pattern Recognition:** While basic UDP and TCP monitoring has been established, the incident revealed the need for deeper, real-time analytics into DNS traffic patterns. This includes volumetric shift detection, DNSSEC processing overhead, and TCP fallback rates. Enhanced dashboards and alert correlation systems should be deployed to provide faster insight during DNS abuse scenarios.

- **National Anycast Deployment for DDoS Isolation:** Reduce dependency on global routing and absorb DDoS pressure closer to the origin by deploying a South African-based Anycast instance. This will lower latency for local queries, increase routing resilience, and help isolate South African traffic from broader volumetric attacks.

- **Operational Preparedness and DDoS Playbook Exercises:** Regularly conduct DDoS-specific response simulations, including desktop and real-time drills. These exercises should validate technical readiness, incident command roles, and external communication protocols under high-pressure conditions.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

- **Strengthen Stakeholder Coordination for Threat Response:** Establish and maintain direct communication protocols with all our external infrastructure operators, including designated DDoS response contacts, escalation paths, and threat intelligence sharing mechanisms. Real-time collaboration channels should be utilised during active events to enhance situational awareness and facilitate a collective response.

Follow-Up Actions

- **DNSSEC Operational Review**: Re-evaluate the current DNSSEC key management lifecycle, including pre-publication, TTL planning, and algorithm agility strategies.
- **Infrastructure Architecture Review**: Reassess the current unicast and Anycast name server deployment to identify and address single points of failure.
- **Threat Intelligence Integration**: Incorporate external threat intelligence feeds to proactively identify and block high-risk IP ranges during future incidents.

Report Approval & Submission

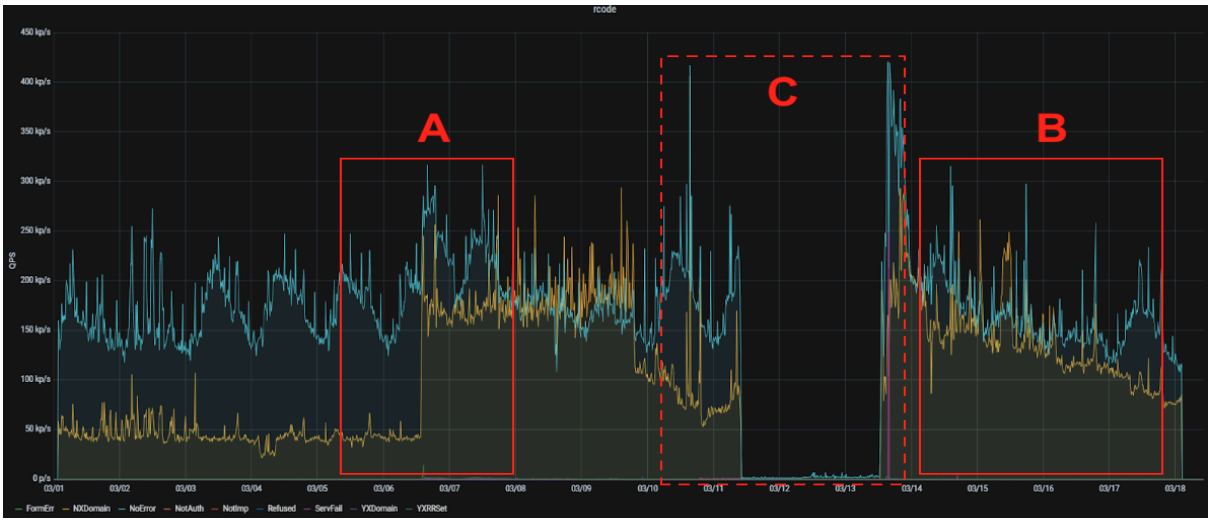
- **Prepared By:** Ed Pascoe (DevOps Manager) & Jerry Maleka (Registry Operations Executive), DevOps Department.
- **Reviewed & Approved By:** Neil Dundas and Lucky Masilela, Co-CEOs, ZARC
- **Date of Limited Distribution (draft):** 25 March 2025
- **Date of Broader Distribution (final):** 20 May 2025

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Schedule 1 - Evidence

Section A: DNS Query and Traffic Volume Charts

Chart A1: RCODE QPS on South African and US Name Servers.



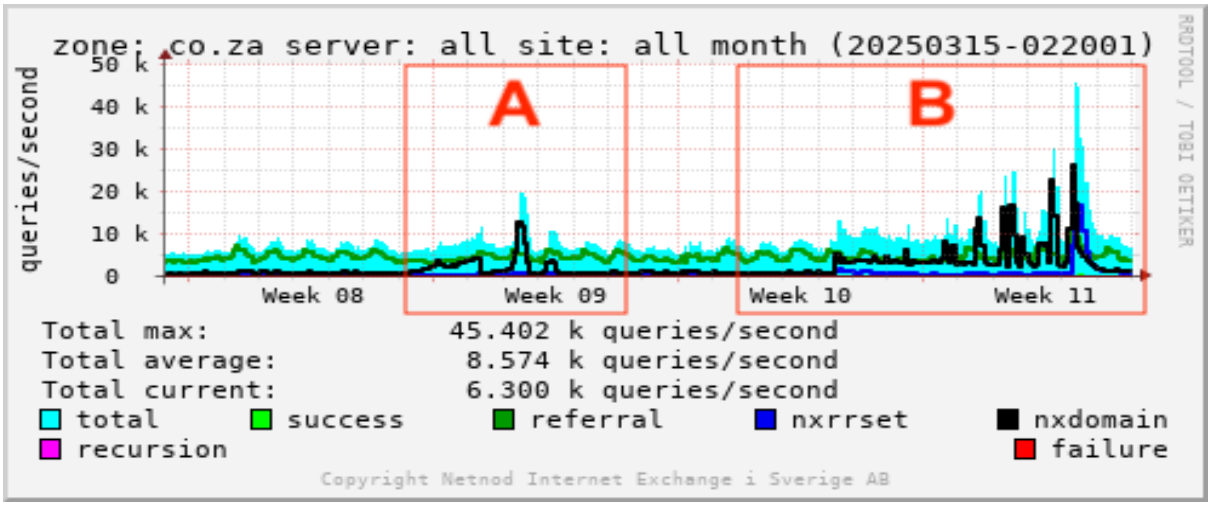
The above chart indicates the RCODE queries per second (QPS) received from the 1st to the 18th of March on **ns.coza.net.za** (South Africa) and **ns2us.dns.business** (USA). The **blue line** indicates NoError (valid) queries, while the **yellow line** indicates NXDomain (non-existent domain) queries.

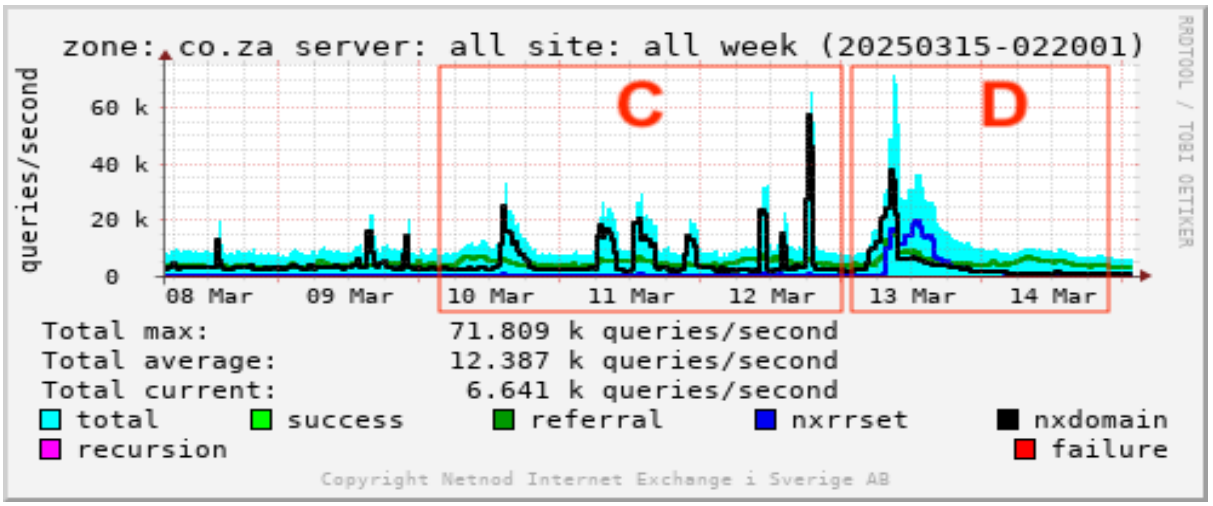
- **Yellow Area Line in Area Labelled "A"**: Indicates a marked and sustained increase in NXDOMAIN (non-existent domain) queries beginning on 6 March, persisting until 10 March when denial-of-service (DoS) mitigation measures began to take effect. While not finally confirmed, the sharp rise and volume of NXDOMAIN responses during this period are consistent with the characteristics of an NXDOMAIN Flood[2]
- **Yellow Area Line in Area Labelled "B":** Following the ZSK Emergency Key Rollover (2048-bit to 1024-bit) on the 13th of March, the NXDomain queries started tapering off, but still remained elevated when compared to the baseline levels observed before the 6th. The system was recovering but still under constant monitoring.
- **Gap Area Labelled "C":** During this period (12th & 13th), the name servers experienced a dramatic spike in DNS queries (Peak DDoS Event). DDoS mitigation included a combination of upstream blackholing, OVH traffic scrubbing and manual interventions from our DevOps team. The sudden spike of malicious traffic overwhelmed parts of the internal monitoring infrastructure, leading to a temporary loss of telemetry data. This accounts for the visible gap in the statistical chart rather than an actual absence of DNS traffic during that period.

[2] Vercara.com Cybersecurity Glossary: DNS NXDomain Attack is a type of Distributed Denial of Service (DDoS) attack that targets both authoritative and recursive (resolver) DNS servers. Attackers flood the server with requests for nonexistent domain names... causing it to waste resources (network, processor, memory, log processing, and storage) on invalid lookups and response - https://vercara.com/resources/glossary-dns-nxdomain-attack

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Chart A2: QPS on the Netnod Anycast System.



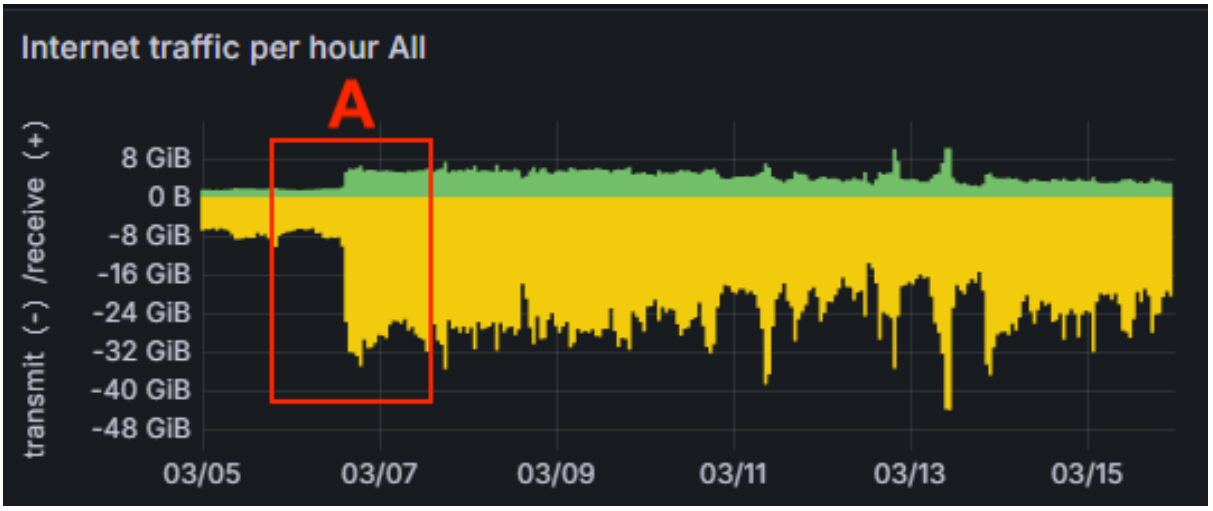


The above charts indicate the queries per second (QPS) received during February and March, for the CO.ZA zone on the Netnod Anycast service, across all sites (nodes).

- **The Area Labelled "A"**: Shows an interesting spike in NXDomain activity (**black line**) during the latter part of February, eventually normalising again in early March.
- **The Area Labelled "B"**: Corroborates the QPS observations of Chart A1 above and shows a clear increase in NXDomain (non-existent domain) queries starting from the 6th of March (**black line**). Note the intermittent spikes in queries for this period.
- **The Area Labelled "C"**: Focuses on the period 10 - 12 March, where there was a substantial increase (intensification) of NXDomain activity. These spikes are suspicious as the NXDomain queries should be small and steady rather than intense spikes.
- **The Area Labelled "D":** Following the ZSK Emergency Key Rollover (2048-bit to 1024-bit) on the 13th of March, the NXDomain queries began tapering off, but NXRRset activity increased for a period. This would indicate that some resolvers could not validate DNSSEC-signed RRsets due to Key Propagation Timing Issues.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Chart A3: Directional Traffic on US Name Server (OVH)

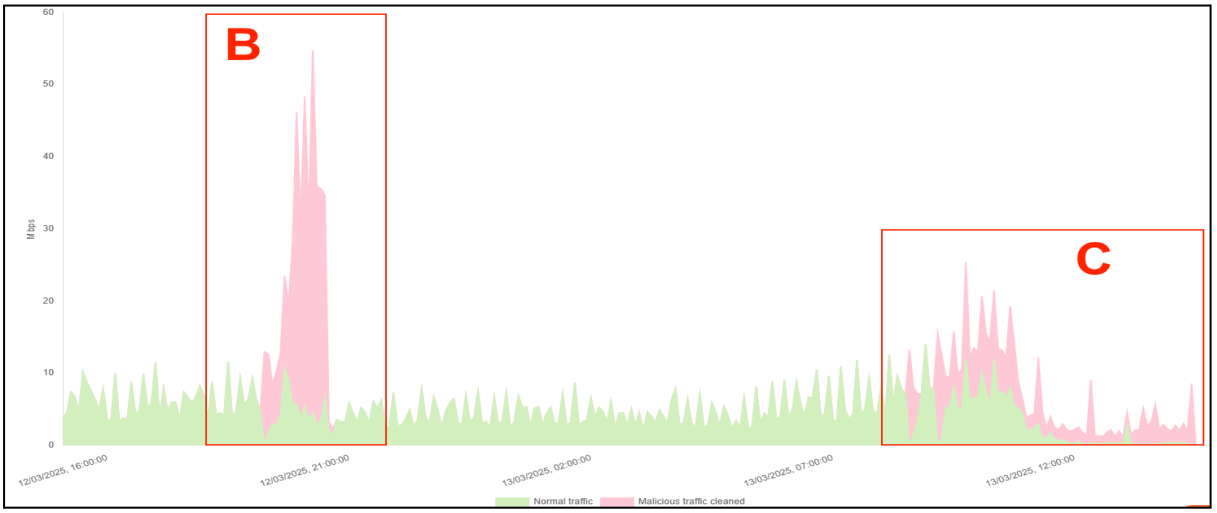


The above chart indicates the Internet Traffic per Hour received and transmitted from the 5th to the 15th of March on the **ns2us.dns.business** (USA) server.

- The **green line** indicates incoming (received) traffic to the server, whilst the **yellow line** indicates outgoing (transmitted) traffic from the server.
- **Before 6 March:** Stable incoming and outgoing traffic consistent with DNS behaviour (i.e. small queries in, larger responses out (with 1024-bit ZSK).
- **Area Labelled "A"**: Shows a clear increase in incoming (received) and outgoing (transmitted) traffic from the 6th of March. Predictably, the yellow line indicates a dramatic increase in outgoing (transmitted) traffic due to larger DNS responses necessitated by implementing the 2048-bit ZSK. The increase in incoming (received) traffic is due to more queries (particularly NXDomain queries). The reasons for the increase in NXDomain query traffic are still unknown (investigation ongoing).
- From the 14th of March onwards, there is a gradual decrease in the incoming (received) and outgoing (transmitted) traffic. This followed the Emergency Key Rollover to a smaller 1024-bit ZSK on the 13th.
- Incoming (received) traffic increased by ~500% after the 6th of March, whereas outgoing (transmitted) traffic increased by ~250% for the same period.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Chart A4: Filtered Traffic on US Name Server (OVH)



The above chart indicates the Filtered Internet Traffic (Mbps) on the **ns2us.dns.business** (USA) server, focusing on 12 - 13 March.

- The **green line** indicates normal traffic, whilst the **pink line** indicates ”malicious traffic cleaned”.
- **Area Labelled “B” (12 March)**: Indicates a sudden and aggressive spike (high-volume flood) in malicious traffic, peaking just above 50 Mbps. Normal (green) traffic appears mostly unaffected and continues steadily below the malicious traffic layer. It would appear that malicious traffic was intercepted (or dealt with) before it could overwhelm the system (i.e. DDoS protection actions).
- **Area Labelled “C” (13 March)**: Indicates a less intense but more prolonged series of malicious traffic bursts, peaking at 25–30 Mbps, with intermittent recurrence. There is noticeable interference with normal (green) traffic, likely caused by upstream DDoS mitigation measures, such as traffic throttling or blackhole routing. This action would likely have affected legitimate query resolution (responsiveness).
- The timing of the malicious traffic surges on the OVH (US) servers coincides with adverse effects recorded on our firewall systems located in South Africa (Teraco). Refer to the charts below.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Section B: Packet Capture showing NXDOMAIN queries

Table B1: Packet Capture - NXDomain with NSEC3

No.	Time	Source	Destination	Protocol	Length	Info
393	0.039059362	131.220.14.204	147.135.106.236	DNS	121	Standard query 0xa4f1 DS 95afuggaqqo5jk9533vtoh35j2dsndh9.co.za OPT
1267	0.108042188	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x3f2e DS cjmvc1945aiegfsmk4knoprcokcej343.co.za OPT
1912	0.162915052	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x7d7e DS 9vk1v09bbtrvgpfabghen09h981l815i.co.za OPT
2329	0.201996602	131.220.14.204	147.135.106.236	DNS	121	Standard query 0x40e2 DS of7o3rra1qila8se0qctd057to8p3tau.co.za OPT
2926	0.266296011	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x7d8a DS 9vk1v09bbtrvgpfabghen09h981l815i.co.za OPT
3615	0.329632572	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x3a7b DS dhg970vbinoamukidcoutluccohscsff.co.za OPT
4635	0.424260511	131.108.163.245	147.135.106.236	DNS	121	Standard query 0xefbc DS dhg970vbinoamukidcoutluccohscsff.co.za OPT
5518	0.498743532	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x47ca DS 7ogf1laimsf5d5jq8tvcme3hdfenn1ij.co.za OPT
6419	0.582237275	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x179e DS 7ogf1laimsf5d5jq8tvcme3hdfenn1ij.co.za OPT
7423	0.668190842	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x6109 DS 5n5rvb4mp93cm613so6c0dv7vvq5k6qc.co.za OPT
8224	0.740578637	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x4423 DS 5n5rvb4mp93cm613so6c0dv7vvq5k6qc.co.za OPT
9265	0.834541456	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x309b DS jc41l8hv01e039k9skcbnpletrb8em1q.co.za OPT
9923	0.896841858	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x435f DS jc41l8hv01e039k9skcbnpletrb8em1q.co.za OPT
11046	1.000674936	131.108.86.82	147.135.106.236	DNS	121	Standard query 0xa8d1 DS i4qi4j42kbpjhmbtg0qgtgngmmje50ci.co.za OPT
11768	1.061118547	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x7859 DS i4qi4j42kbpjhmbtg0qgtgngmmje50ci.co.za OPT
12921	1.171088218	131.108.86.82	147.135.106.236	DNS	121	Standard query 0xe9dc DS d7u9965fu2jgt9l81gc7865easjttsqk.co.za OPT
13571	1.219214917	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x5916 DS d7u9965fu2jgt9l81gc7865easjttsqk.co.za OPT
14979	1.344302416	131.108.86.82	147.135.106.236	DNS	121	Standard query 0xdffa DS au2i9k1lpprrlhvfj9qe6jpjksl1j0hh.co.za OPT
15386	1.381095799	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x065f DS au2i9k1lpprrlhvfj9qe6jpjksl1j0hh.co.za OPT
15988	1.431704461	130.73.120.190	147.135.106.236	DNS	121	Standard query 0x966d DS geil3ijvpj10jh0uqckknetlalrecftp.co.za OPT
16839	1.507528763	131.108.86.82	147.135.106.236	DNS	121	Standard query 0xaebb DS gr3eutn2gjlki7dm1vud7piog0q0vk67.co.za OPT
17276	1.542685126	131.108.163.245	147.135.106.236	DNS	121	Standard query 0x379e DS gr3eutn2gjlki7dm1vud7piog0q0vk67.co.za OPT
17964	1.602044508	130.73.120.190	147.135.106.236	DNS	121	Standard query 0x46af DS 9m8pvf9jk87he4jte8pknh4pp4ijdcs7.co.za OPT
18822	1.674326487	131.108.86.82	147.135.106.236	DNS	121	Standard query 0x770f DS 03jcuifn2cfteuplhfe3t06pfhr2d3pv.co.za OPT
19165	1.706062244	131.108.163.245	147.135.106.236	DNS	121	Standard query 0xec94 DS 03jcuifn2cfteuplhfe3t06pfhr2d3pv.co.za OPT
19969	1.779866045	130.73.120.190	147.135.106.236	DNS	121	Standard query 0xee6c DS ul56qba9if3hd53ts1u1suf65vadktca.co.za OPT

Packet Capture Analysis (16 March): The above table presents a filtered subset of DNS query traffic collected during a targeted packet capture on March 16, 2025, on the ns2us.dns.business (US) authoritative name server. The data was refined to focus on queries likely to return NXDOMAIN responses, specifically queries for non-existent (bogus) CO.ZA domain names that request DNSSEC data, particularly DS records.

The purpose of this sample is to characterise the suspicious DNS traffic observed under elevated load conditions and to identify any common patterns in query origin or intent.

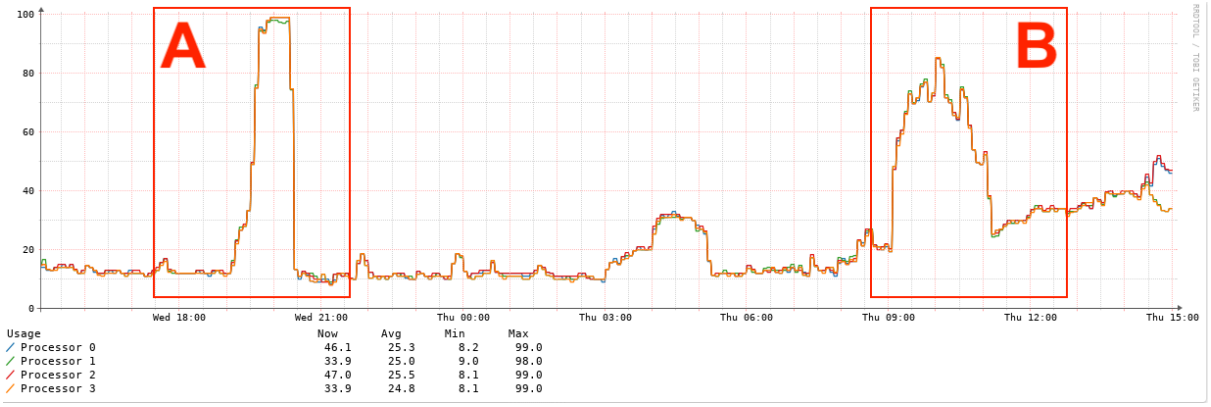
The packet capture analysis confirms that a significant portion of the suspicious traffic received on March 16, 2025, consisted of algorithmically generated, non-existent CO.ZA domain queries requesting DNSSEC-enabled DS records. These queries are designed to elicit expansive NXDOMAIN responses, consuming disproportionate server resources and aligning with known characteristics of a DNS-based denial-of-service attack.

The presence of recurrent queries from seemingly spoofed or untrusted source IPs (originating from multiple networks and geographic regions) further supports the conclusion that the traffic was not legitimate.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Section C: System Resource Utilisation Charts

Chart C1: ZARC Core Firewall (Teraco) - Processing Resources



The above chart tracks processor demand on the ZARC core firewall, hosted at Teraco (Johannesburg), focusing on the 12th (Wednesday) and 13 (Thursday) March.

- **Area Labelled "A" (Wednesday, 12 March)**: During this window, CPU utilisation across all four processors spiked sharply, reaching near-maximum saturation (~99%). This period aligns with a surge in malicious traffic to other authoritative name servers (refer to chart A4, area B above), particularly characterised by NXDOMAIN responses and increased DNSSEC overhead. The elevated processing load suggests that the firewall was actively inspecting and filtering high volumes of inbound traffic, consistent with a DNS-based denial-of-service (DoS) event.

- **Area Labelled "B" (Thursday, 13 March)**: A second significant CPU load event occurred the following morning, peaking around 80–90% across all cores. This aligns with a second wave of elevated malicious traffic (refer to chart A4, area C above). While slightly lower in intensity than the first, the sustained processor load again indicates a period of significant strain on the firewall system, likely due to continued or evolving DoS activity targeting DNS infrastructure.

- Between and after these peaks, CPU usage returns to baseline levels (~10-20%), suggesting that the firewall normally runs with ample headroom. The marked spikes observed during the incident are anomalous and strongly correlate with the timing and nature of the malicious traffic surges observed on the OVH (US) server. There is a strong correlation between CPU load and query volume in previous DNS data, indicating that the firewall is the primary choke point for inbound DNS traffic to the Teraco-based authoritative name servers.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Post-Incident Update (July 2026)

Since the original distribution of this report, further operational and technical work has been undertaken to strengthen the resilience of the .ZA Shared Registry System (SRS) and to implement the lessons identified during the post-incident review.

Key developments include:

1. Continued Technical Analysis

   Additional review of operational telemetry and packet captures further supports the conclusion that the principal driver of the incident was an abnormal surge in NXDOMAIN query traffic consistent with an NXDOMAIN flooding (DNS water torture) attack. While the DNSSEC key size change contributed to increased response sizes and operational pressure, it is not considered the primary initiating cause of the incident.

   As part of the post-incident review, the response team also consulted internationally recognised DNS experts with extensive operational experience in managing root server infrastructure, country code Top-Level Domains (ccTLDs), and other large-scale authoritative DNS environments. While no definitive technical mechanism could be identified to explain the timing of the abnormal increase in NXDOMAIN query traffic, the subsequent analysis supports the possibility that the DNSSEC infrastructure change may have been observed and opportunistically exploited by external actors. Although this cannot be confirmed conclusively, the available evidence suggests that the abnormal query activity was unlikely to have been entirely coincidental. The precise motivation and origin of the activity remain unknown.

2. DNS Infrastructure Improvements

   The registry has continued to enhance the resilience of its authoritative DNS infrastructure through additional capacity upgrades, architectural improvements and refinement of operational procedures. These improvements have increased operational resilience, reduced dependency on individual infrastructure components and improved readiness for future high-volume traffic events.

3. DDoS Mitigation Enhancements

   Detection, monitoring and response capabilities have been strengthened through improved traffic analysis, operational playbooks and closer coordination with infrastructure providers.

4. National Anycast Initiative

   One of the principal recommendations arising from the incident was the deployment of additional local authoritative DNS capacity within South Africa.

   A prototype national authoritative Anycast framework has been established and continues to undergo operational testing prior to phased production deployment. The objective is to improve service resilience, reduce latency for South African users and distribute authoritative query load more effectively across the national infrastructure.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved

Operational Procedures

DNSSEC key management procedures, infrastructure change controls and incident response processes have all been reviewed and enhanced to reduce operational risk during future maintenance activities.

The recommendations arising from this incident have either been implemented or incorporated into the registry's ongoing technical roadmap and operational planning. ZARC remains committed to continuous improvement, operational transparency and sharing technical experience with the broader Internet community in support of a more resilient South African and global DNS ecosystem.

© 2025-2026 ZA Registry Consortium (Pty) Ltd. All Rights Reserved