

# Report for ccNSO Council

TechDay ICANN 77, Washington, DC

**Eberhard W Lisse**

Nambian Internet Services (Pty) Ltd

[dns-admin@na-nic.com.NA](mailto:dns-admin@na-nic.com.NA)

2023-06-13

## **Eberhard Lisse**

### **Opening Remarks**

As per usual I introduced the session agenda. One presentation arrived late so it could not be accommodated, but was earmarked for the next (Hamburg) meeting.

## **Giovane C. M. Moura (remote)**

### **E-Gov DNS infrastructure**

NCSC-NL commissioned SIDN Labs for a study on Dutch e/gov DNS resilience (the DINO project). Triggered by a hacker attack on several .gov domains in USA. It measured whether the e-gov DNS infrastructure is configured according to the best practices and compared with e-gov domains of .se, .ch and .gov.

Measured were

- the number of DNS providers,
- prefix diversity,
- number of TLDs,
- use of Anycast, and
- the TTL setup.

## **Alain Durand (remote)**

### **DNSSEC Concentration & Deployment in SLDs**

They used the *Majestic Million* list and checked different slices of this group – small vs large etc. The study looked at who was using which DNS servers. The study also checked SLDs in top 25 TLDs for DNSSEC deployment. Some TLDs seem to have zero DNSSEC deployment.

## **Mark Elkins – (remote)**

### **CDS Scanning & Other Consistency Checks**

First, Mark explained how to add DNSSEC to a zone. Then he introduced his PHP script for CDS scanning. It is used to add DS records to the edu.za zone which is under his management. DS records are added if CDS remains unchanged for 3 consecutive days.

## **Andy Newton**

### **New ICANN RDAP Tools**

ICANN mandates that RDAP will be the replacement for WHOIS in the gTLD space. They wrote a Command Line Client in Rust. It has an API to connect with Jcard. It is open source, published on Github.

The goals are to

- create native python bindings,
- be an experimental platform, and
- enable RDAP-based research.

The experience from writing a client helps with understanding the server. Andy also mentioned Client Extension Signaling. Several server issues were found during the development of the client.

## **Garth Miller (remote)**

### **CoCCATools Update**

Garth introduced new improvements in the upcoming version of CoCCA:

- Portal update (mobile friendly),
- improved resiliency
- replication monitoring,
- RDAP module,
- DNS abuse monitoring,
- EPP updates to support DS record management,
- module to support blocking initiatives

## **Rob Seger**

### **Malware Obfuscation**

Rob introduced two attackers' advantages:

1. Hackers have the detection SW, and they even often have an access to the source of it.
2. PHP language is a problem itself.

Then showed how to obfuscate a code to run an external command. He also showed how ChatGPT AI can help attackers by further obfuscating malicious code.

## **Mats Dufberg (remote)**

### **Zonemaster of Scale**

Mats talked about checks on the .se zone using their Zonemaster tool. Zonemaster was designed for single tests,

- it checks delegation,
- verifies nameservers for consistent responses,
- verifies they respond to queries, and
- verifies DNSSEC.

It is an open-source tool, available on Github and supports several languages. In March .se ran a test for all 1.5 million domain names in the zone. All in all 72 tests were run per domain name which took 5 days. 7% of domain had issues that made impossible to finish a test. Then Mats went through the common errors and warnings. Zonemaster has GUI and CLI interfaces and can be run on Docker.

## **Ondřej Filip**

### **Closing remarks**

Ondřej summarized all presentations and thanked the speakers and also the chair “for preparing yet another interesting session”.

This report draws heavily on his notes for which I am grateful.

## **Eberhard Lisse**

### **TechWG summary**

I quickly went through two slides about past TechDays that will be presented at the ccNSO meeting in DC.