

Technical Quarterly Report –Apr 2020 - Jun 2020

BASIC PROGRAMMATIC DATA

Performer: University of Twente

Project: 628.001.031(NWO)

Mapping Domain DNS DDoS Vulnerabilities to Improve Protection and Prevention

Period of Performance (base): December 1, 2018 – November 30, 2022

PROJECT PROGRESS

Progress Against Planned Objectives:

Paper on delegation inconsistency presented at RIPE80.

(https://www.caida.org/catalog/media/2020_when_parents_children_disagree_pam/when_parents_children_disagree_pam.pdf)

Paper on orphan and abandoned records accepted to WTMC2020

(<https://indico.dns-oarc.net/event/34/contributions/794/attachments/762/1292/OARC33.pdf>)

Two Papers submitted at IMC2020

Attended at RIPE80 workshop

Monthly conference calls between UT and CAIDA are taking place to discuss the project progress.

Technical Accomplishments this Period: Developed a tool for detection of DNS parent-children misconfiguration in a controlled environment (<https://superdns.nl/>)

DNS-OP is designing an Internet draft to address the problem of parent-children to which we are trying to contribute with our work <https://tools.ietf.org/html/draft-huque-dnsop-ns-revalidation-01>

Improvements to Prototypes this Period: Providing insight to the operators and users through <https://superdns.nl/> as a first step of MADDVIPR Framework.

Significant Changes to Technical Approach to Date: none

Deliverables: Develop strategies to make OpenINTEL data available via IMPACT

Technology Transition and Transfer this Period: none

Publications this Period:

- **The Forgotten Side of DNS: Orphan and Abandoned Records (WTMC2020)**
- **MANycast2 -- Using Anycast to Measure Anycast: Challenges and Opportunities (IMC2020)**
- **Unresolved Issues: Prevalence, Persistence, and Perils of Lame Nameservers (IMC2020) (External Collaboration)**

Meetings and Presentations this Period: RIPE80, CONCORDIA Early Stage PhD Workshop

Issues or Concerns: none

PROJECT PLANS

Planned Activities for Year 2:

- UT and CAIDA will study the network layer architecture of the DNS, in order to identify SPoF and aggregation points in the global DNS infrastructure.

- Using the data provided by OpenINTEL and combining it with other sources UT will identify possible weak points and future attacks.

Specific Objectives for Next Period:

UT and CAIDA will work on studying the DNS Anycast deployment