

Technical Quarterly Report –Jan 2019 - Mar 2019

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 31, 2022

PROJECT PROGRESS

Progress Against Planned Objectives:

UT performed an analysis of State of the Art of DNS vulnerabilities and DNS DDoS attack.

UT submitted a poster proposal that has been accepted for presentation at ICT.OPEN 2019 Conference.

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

Technical Accomplishments this Period:

We created a project web site:

<https://maddvipr.org/>

Deliverable and monthly reports will be made available at

<https://maddvipr.org/deadline/>

Improvements to Prototypes this Period: none

Significant Changes to Technical Approach to Date: none

Deliverables:

- Y1:M3 - Background research on DNS vulnerabilities

Technology Transition and Transfer this Period: none

Publications this Period:

- MADDVIPR Poster accepted at ICT.OPEN 2019 Conference.

Meetings and Presentations this Period: none

Issues or Concerns: none

PROJECT PLANS

Planned Activities for Year I:

- UT will investigate the state of the art of DNS DDoS vulnerabilities and Misconfiguration.
- 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 will investigate the parent/child delegation TTL and NS mismatches by identifying the spread of the phenomenon, the impact on the resilience against DDoS attacks and DNS hijacking, and possible solution to the problem.