

Technical Quarterly Report –Apr 2019 - Jun 2019

BASIC PROGRAMMATIC DATA

Performer: CAIDA, University of California San Diego (UCSD)

Project: DHS S&T cooperative agreement FA8750-19-2-0004

Mapping Domain DNS DDoS Vulnerabilities to Improve Protection and Prevention

Period of Performance (base): November 1, 2018 – October 31, 2022

Total Award Value: \$250,000

PROJECT PROGRESS

Progress Against Planned Objectives:

UT has investigated the parent/child delegation TTL and NS mismatches by identifying the spread of the phenomenon, the software behavior and possible solution to the problem.

UT submitted and presented a poster to TMA 2019 Paris about TTL Mismatches.

UT has investigated the orphan DNS records problem.

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

Technical Accomplishments this Period: none

Improvements to Prototypes this Period: none

Significant Changes to Technical Approach to Date: none

Deliverables: none

Technology Transition and Transfer this Period: none

Publications this Period:

- It's Time to Lie: The DNS TTL Mismatch Problem. Poster presented at TMA 2019 Paris

Meetings and Presentations this Period: none

Issues or Concerns: none

PROJECT PLANS

Planned Activities for Year I:

- UT and CAIDA 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 and CAIDA will expand the work on the parent/child delegation TTL and NS mismatches by analyzing the large-scale impact through RIPE Atlas.

UT and CAIDA will continue the work on orphan records and will submit a poster to IMC 2019 Reproducibility Track. A paper as an extended version of the poster will also be considered.