Technical Quarterly Report –Oct 2020 - Dec 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 MAnycast2 presented at IMC2020
Attended at IMC2020 conference
(https://indico.dns-oarc.net/event/34/contributions/794/attachments/762/1292/OARC33.pdf)
Blog Post on MAnycast2 on APNIC
Monthly conference calls between UT and CAIDA are taking place to discuss the project progress.

Technical Accomplishments this Period:

1. We presented a methodology for detecting Anycast prefixes (Manycast2). https://www.caida.org/catalog/media/2020_manycast2_imc/manycast2_imc.pdf
2. We wrote a blog post regarding it at APNIC. https://blog.apnic.net/2020/12/15/manycast2-using-anycast-to-measure-anycast/
3. We registered orphan records and we are actively intercepting their traffic, in order to perform analysis on the nature of the content hosted by these records. (Privacy sensitive, URL not reported)
4. We showed the capabilities of DNSAttackStream in an internal event for the Netherlands National Cyber Security Centre (NCSC-NL), proving its ability to identify an attack to a large Dutch DNS provider and showing the impact of the attack on the DNS. (Privacy sensitive, URL not reported)

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:

- **MAnycast2 -- Using Anycast to Measure Anycast (IMC2020) - Presented**
- **Unresolved Issues: Prevalence, Persistence, and Perils of Lame Delegation (IMC2020) (External Collaboration) - Presented**

Meetings and Presentations this Period: IMC2020
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 the impact of DDoS attacks against DNS.

Specific Objectives for Next Period:

UT and CAIDA will work on studying the DNS Anycast deployment
UT and CAIDA will work on studying the DNS Orphan Traffic