Technical Quarterly Report –Jul 2020 - Sep 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 orphan and abandoned records presented to WTMC2020
Paper on orphan and abandoned records presented to OARC33
(https://indico.dns-oarc.net/event/34/contributions/794/attachments/762/1292/OARC33.pdf)
Two Papers accepted at IMC2020
Attended at OARC33 workshop
Monthly conference calls between UT and CAIDA are taking place to discuss the project progress.

Technical Accomplishments this Period:

1. We developed a methodology for detecting Anycast prefixes (Manycast2). We will use it to analyze Anycast deployment in the DNS. https://github.com/ut-dacs/Anycast-Census
2. Afilias acknowledge us for helping to identify the orphan records misconfiguration and take action to fix it. http://www.circleid.com/posts/20200811-afilias-to-protect-tlds-against-potential-orphan-glue-exploits
3. We developed the prototype of DNSAttackStream. The software joins the live RSDOS (Reflected Spoofed Denial of Service) attacks data provided from CAIDA Network Telescope with live DNS measurement performed by OpenINTEL. DNSAttackStream will allow us to understand the impact of DoS attacks against DNS infrastructure. http://192.87.172.248:3000/d/AOK3LzVMk/dnsattackstream?orgId=1

Improvements to Prototypes this Period: none
Significant Changes to Technical Approach to Date: none
Deliverables: Design and prototype DNSAttackStream
Technology Transition and Transfer this Period: none
Publications this Period:

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

Meetings and Presentations this Period: WTMC2020, OARC33
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