Denial-of-Service Open Threat Signaling (DOTS) Telemetry

https://tools.ietf.org/html/draft-reddy-dots-telemetry-04

IETF 106, Singapore

Nov 2019

Presenter: T. Reddy (McAfee)

M. Boucadair (Orange)

E. Doron (Radware)

M. Chen (China Mobile)

Agenda

- Major updates from 01 to 03 to address the comments from the WG and to integrate draft-chen-dots-attack-informations-03 draft
- Questions & Comments

DOTS Telemetry

- "DOTS Telemetry" is defined as the collection of attributes characterizing the normal baseline and actual attack, and both are useful for DDoS detection and mitigation.
  - The DOTS Telemetry is an optional set of attributes that can be signaled in DOTS signal and data channel protocols.

DOTS Telemetry

- Added path suffix “/telemetry” to signal the DOTS telemetry.

Total connections capacity

- Baseline for resource consuming DDoS attack for a target per transport protocol
  - Max number of simultaneous connections that are allowed to the target server.
  - The maximum number of simultaneous connections that are allowed to the target server per client.
  - The maximum number of simultaneous embryonic connections that are allowed to the target server.
  - The maximum number of simultaneous embryonic connections that are allowed to the target server per client.
  - The maximum number of connections allowed per second to the target server.
  - The maximum number of connections allowed per second to the target server per client.

Total connections capacity (cont.)

- Baseline for resource consuming DDoS attack for a target per transport protocol
  - ➢ The maximum number of requests allowed per second to the target server.
  - ➢ The maximum number of requests allowed per second to the target server per client.
  - ➢ The maximum number of partial requests allowed per second to the target server.
  - ➢ The maximum number of partial requests allowed per second to the target server per client.

Total attack connections

- Low, medium, high and peak percentile for
  - The number of simultaneous attack connections to the target server.
  - The number of simultaneous embryonic connections to the target server.
  - The number of attack connections per second to the target server.
  - The number of attack requests to the target server.

Attack Details

- Attack details can be signaled from the DOTS client to DOTS server and vice-versa.
  - For example, DOTS server co-located with a DDoS detector signals the attack details to the DOTS client.
  - Asynchronous notifications of the attack details using Observe Option
- Updated Attack details with the following attributes
  - start-time
  - end-time
  - Count of sources involved in the attack
  - Bandwidth or resource consuming DDoS attacks and corresponding attack attributes per target.
  - List of top talkers targeting the victim and the attack traffic from each of the top talkers
    - Top talkers are spoofed IP addresses (e.g., reflection attacks) or not.
    - Bandwidth or resource consuming DDoS attacks and corresponding attack attributes per talker.

DOTS Telemetry configuration

- Negotiate the configuration parameters for the telemetry data (e.g., low, mid, or high percentile values).

Other changes

- Added YANG module
- CBOR mapping registry

Discussion

- Some telemetry like baseline and connection capacity can be communicated using DOTS data channel.
  - ❑ Do we need both protocols for DOTS telemetry ?
- Any other configuration parameters to be negotiated by DOTS client and server ?

draft-reddy-dots-telemetry-04

- Comments and suggestions are welcome
- Request for WG adoption