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

https://tools.ietf.org/html/draft-reddy-dots-telemetry-01

IETF 105, Montreal

July 2019

Presenter: T. Reddy (McAfee)

M. Boucadair (Orange)

E. Doron (Radware)

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.
- (RFC8612) GEN-004 Mitigation Hinting:
    - DOTS clients MAY send mitigation hints derived from attack details to DOTS servers, with the full understanding that the DOTS server MAY ignore mitigation hints.
    - DOTS-server handling of mitigation hints is implementation-specific.
- https://tools.ietf.org/html/draft-doron-dots-telemetry-00 was presented in IETF-97.
    - WG decided to look into it after the DOTS protocol work is complete.

Need for DOTS Telemetry

- “normal traffic baseline” learned and constructed by DOTS telemetry is indispensable for "anomaly detection" approach of attack detection
- A single DOTS client may not have complete knowledge for an attack, the DOTS server receiving DOTS telemetry from multiple DOTS clients has better visibility in comparison.
- DOTS telemetry is useful to get visibility into the DDoS attack, hence to improve greatly the mitigation performances in terms of time to mitigate, accuracy, false-negative, false-positive, and other measures
- Modern attacks are complicated, multi-vectored and mutable, comprehensive knowledge is highly desirable.
- Mutual DOTS telemetry sharing between DOTS agents is crucial for "closing the mitigation loop“ to better alignment.

DOTS Telemetry use case

- In case of attack happens and cannot be mitigated by enterprise DMS itself, the DOTS client signals the need for aid in mitigating the on-going attacks from the MSP’s DOTS server
    - the MSP can use the DOTS Telemetry it received from the DOTS client to get visibility, and assign the adequate mitigation resources, tune the mitigators with the normal baseline, assign the appropriate personnel to handle the enterprise attacks, and so forth.

Pre-mitigation Telemetry Attributes

- Some of the Pre-mitigation attributes can signaled during peace time either using the DOTS signal or data channel
  - Total Traffic Normal Baseline : The low percentile (10th percentile), mid percentile (50th percentile), high percentile (90th percentile) and peak values measured in PPS/Kpps, BPS, Kbps/Mbps/Gbps
  - Total Pipe Capacity
- When DDoS attack is detected and mitigation is requested
  - Total Attack Traffic
  - Total Traffic
  - Attack Details
    - Vendor-ID : Security vendor’s Enterprise number registered with IANA.
    - Attack-ID: Unique attack identifier assigned by the vendor.
    - Attack-Name: Attack description
    - Attack-severity: Emergency (0), critical (1) and alert (2).

Mitigation Efficacy attributes

- Total Attack Traffic
- Attack details
    - Vendor-ID
    - Attack-ID
    - Attack-Name
    - Attack-severity

Mitigation status attributes

- List of attacks detected by the countermeasure mechanisms.

draft-reddy-dots-telemetry-01

- Comments and suggestions are welcome