# Distributed Denial-of-Service Open Threat Signaling (DOTS) Telemetry Specifications
# draft-doron-dots-telemetry-00


| | |
|---|---|
| Ehud Doron | Radware |
| Tirumaleswar Reddy, Flemming Andreasen | Cisco |
| Liang Xia | Huawei |
| Kaname Nishizuka | NTT |


November2016 Seoul

# What is DOTS Telemetry

- **DOTS Telemetry**

  "DOTS Telemetry" is defined as the collection of attributes characterizing the actual attacks and normal baseline, both are useful for DDoS detection and mitigation. The DOTS Telemetry is an optional set of attributes that can be signaled in the various DOTS protocol messages.

- **Constraints**
  - Optional, not mandatory
  - Hints, not compulsory
  - Do not influence DOTS signal's reliability and efficiency

# Why is DOTS Telemetry Needed

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

# Examples of DOTS Telemetry Attributes

- Pre-mitigation DOTS Telemetry attributes
  - "Normal Baselines" of legitimate traffic
  - "Total Attack Traffic volume“
  - "Attack Details“: [CEF] definition
  - "Total pipe capacity“
  - List of already "Authenticated source IPs"
- C2S Mitigation Status DOTS Telemetry attributes
  - Current "Total traffic volumes“
  - Current "Total Attack Traffic“
  - "Mitigation Efficacy Factor“
  - "Attack Details“
- S2C Mitigation Status DOTS Telemetry attributes
  - Current "Mitigation Countermeasure status"

**Modularity, Extensibility, Sufficiency**

# DOTS Telemetry Use Cases

- Hybrid anti-DoS services use-case
  - During peace time, the enterprise mitigators build the enterprise protected service's normal baseline
  - In case of attack happens and cannot be mitigated by enterprise itself, the DOTS Client signals the need for aid in mitigating the on-going attacks from the MSP's DOTS Server
  - In order to fulfill his SLA, the MSP uses the DOTS Telemetry it received from the 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.
- MSP to MSP anti-DoS services use-case: similar to above use case, DOTS telemetry is also needed!

# Summary

- Objective: bring the DOTS telemetry to the WG for discussion:
  - various needs and means
  - How to use them for optimized mitigation
  - Differentiate between baseline capability from extensions

- Suggestion:
  - DOTS WG use cases draft is not sufficient in describing DOTS telemetry use case, more contents can be added to enrich with Telemetry related items
  - A separate DOTS telemetry draft is a good way to support the DOTS protocol draft with future extensibility

# Thanks!

Liang Xia (Frank)