PoC report of intra-domain DDoS Orchestration usecase in draft-ietf-dots-use-cases-12

Yuhei Hayashi, Takeaki Nishioka (NTT Network Service Systems Labs) 
{hayashi.yuhei, nishioka.takeaki}@lab.ntt.co.jp
Summary

- We have demonstrated a PoC of intra-domain use case using go-dots.
- We would like DOTS Clients to send attacker’s info (e.g. top talker).
Motivation

- We would like to **automate DDoS Mitigation** in intra-domain NW with an Orchestrator.
- We also would like to try DOTS as **standardized IF** between the Orchestrator and (Flow collectors | DDoS Mitigation Systems).

This automates ...
- Collecting information
- Deciding what to do
- Ordering to mitigate
Report: PoC Overview

Our PoC use case

Flow collector

Orchestrator

DMS

PE Router

DDoS Orchestration

Draft-ietf-dots-use-cases-12

Admin

Collector

Orchestrator

DMS

PE Router

Flow

Analyze

Mitigate

Mitigate

Mitigate

* C is for DOTS client functionality
* S is for DOTS server functionality

DOTS Signal
(Mitigation Request)

BGP (Redirect)

DOTS Signal
(Offload Request)

BGP (RTBH)
Report: Action 1/5

Action #1: Send netflow to flow collector
Report: Action 2/5

**Action #2-1:**
*(When volume attack is detected)*
Request DDoS Mitigation

**Action #2-2:**
Extract target ip address from the syslog and transform it into input of go-dots client controller.

**Action #2-3:**
Send DOTS signal
**Report: Action 3/5**

1. **DOTS Client VM for flow collector**
   - Fluentd
   - Flow collector Plugin

2. **DOTS Client VM for vAPS**
   - vAPS Plugin
   - Fluentd

3. **DOTS Server VM**
   - go-dots Client
   - go-dots Server

**Action #3-1:** Invoke goBGP

**Action #3-2:** Redirect attack traffic to DDoS Mitigation Systems

**PE Router (MX104/Juniper)**

**PE Router (7750 / Nokia)**

**Pseudo attacker (IXIA)**

**Pseudo target (IXIA)**

**Core NW**

**Flow collector**

**Scrubbing Center**

**Orchestrator**

**DDoS Mitigation System (vAPS / Arbor)**

**GRE Endpoint Router (ASR1009 / Cisco)**
Report: Action 4/5

Action #4-1: (When attack is detected) Mitigation offload request

Action #4-2: Extract target ip address and transform it into input of go-dots client controller.

Action #4-3: Send DOTS signal
**Report: Action 5/5**

**DOTS Client VM for flow collector**
- Flow collector Plugin
  - Fluentd
- go-dots Client Controller
- go-dots Client

**DOTS Client VM for vAPS**
- vAPS Plugin
  - Fluentd
- go-dots Client Controller
- go-dots Client

**DOTS Server VM**
- go-dots Server
- go-dots Server

**Action #5-1: Invoke goBGP**

**Action #5-2: RTBH by BGP**

- Pseudo attacker (IXIA)
- PE Router (MX104/Juniper)
- PE Router (7750 / Nokia)
- Pseudo target (IXIA)
- Core NW
- Flow collector
- Orchestrator
- Scrubbing Center
- DDoS Mitigation System (vAPS / Arbor)
- GRE Endpoint Router (ASR1009 / Cisco)
Requirement:

We want DOTS Clients to send attacker information (e.g. top talker) to block attack traffic at PE routers more correctly.
Discussion

- Does our PoC use-case attract you?
- If it does, what do you think about our requirement?