DDoS mitigation offload use-case and YANG module expansion in signal channel
draft-h-dots-mitigation-offload-expansion-00

Yuhei Hayashi / NTT
Kaname Nishizuka / NTT Communications
Summary

- We wrote an I-D about DDoS mitigation offload use-case and signal channel expansion based on our report at IETF102.

- We extended YANG module of signal channel so that DOTS can send attacker information (top talker).
Our report at IETF102

Features
- Intra-domain DDoS Orchestration
- Using go-dots

Action
- Detect DDoS at the Flow collectors
- Redirect attack traffic to DMS
- Detect DDoS at DMS
- RTBH at PE routers
Our report at IETF102

Requirement:
We want DOTS Clients to send attacker information (e.g. top talker) to block attack traffic at PE routers more correctly.
Feedback from WG

[Feedback]
- The signal channel should be frozen at a certain point.
- DOTS WG can do some extensions after the core things are done.

[Our Impression]
Signal-channel’s WG state: “Submitted to IESG for Publication”. It is good time to discuss some extension of signal channel in WG.

[Feedback]
- Please write a draft.

[Our work]
We’ve written a new I-D about the extension.
Summary of the draft
Use-case: Component diagram

draft-h-dots-mitigation-offload-expansion-00
draft-ietf-dots-use-cases-16

The difference
- DMS have a client function
- Routers/Switches collaborate
**Summary of the draft**

**Use case: Sequence diagram**

* C is for DOTS Client functionality
* S is for DOTS Server functionality

**DDoS offload action**

(It offloads mitigation from DMS to Routers/Switches.)
The augment statement allows a module or submodule to add to a schema tree defined in an external module, or in the current module and its submodules, and to add to the nodes from a grouping in a uses statement."  

[RFC7950 The YANG 1.1 Data Modeling Language]
Summary of the draft
Extension of Signal Channel (Content)

draft-h-dots-mitigation-offload-expansion-00

module ietf-dots-signal-channel-mitigation-offload-expansion {
  yang-version 1.1;

  namespace "urn:ietf:params:xml:ns:yang:
    ietf-dots-signal-channel-mitigation-offload-expansion";

  ...

  /*
   * Groupings
   */
  grouping attacker {
    description
      "Specifies the attackers of the mitigation request.";
    leaf-list attacker-top-talkers-prefix {
      type inet:ip-prefix;
      description
        "IPv4/IPv6 prefix identifying the top-talker in attackers.";
    }
  }

  /*
   * Main Container for DOTS Signal Channel Expansion
   */
  augment "/signal:dots-signal/signal:scope/"{
    uses attacker;
  }
}