DOTS M. Chen
Internet-Draft Li. Su
Intended status: Informational Jin. Peng
Expires: January 7, 2020 CMCC
July 06, 2019

A method for dots server deployment
draft-chen-dots-server-hierarchical-deployment-00

Abstract

As DOTS is used for DDoS Mitigation signaling, In practice, there are different deployment scenarios for DOTS agents deployment depending on the network deployment mode. This document made an accommandation for DOTS Server deployment which may be Suitable for ISP. The goal is to provide some guidance for DOTS agents deployment.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

DDoS Open Threat Signaling (DOTS) is a protocol to standardize real-time signaling, threat-handling requests[I-D.ietf-dots-signal-channel], when attack target is under attack, dots client send mitigation request to dots server for help, If the mitigation request contains enough messages of the attack, then the mitigator can respond very effectively.

In the architecture draft[I-D.ietf-dots-architecture], it is says that this does not necessarily imply that the attack target and the DOTS client have to be co-located in the same administrative domain, but it is expected to be a common scenario. Although co-location of DOTS server and mitigator within the same domain is expected to be a common deployment model, it is assumed that operators may require alternative models.

In the DOTS server discovery draft[I-D.ietf-dots-server-discovery], it is says that a key point in the deployment of DOTS is the ability of network operators to be able to onfigure DOTS clients with the correct DOTS server(s) nformation consistently.

In the DOTS multihoming draft[I-D.ietf-dots-multihoming], it provides deployment recommendations for DOTS client and DOTS gateway, it is says when conveying a mitigation request to protect the attack target, the DOTS client among the DOTS servers available Must select a DOTS server whose network has assigned the prefixes from which target prefixes and target IP addresses are derived. This implies that id no appropriate DOTS server is found, the DOTS client must not send the mitigation request to any DOTS server. So in this document,

we give some dots server deployment consideration as the title suggests we prefer hierarchical deployment.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

The readers should be familiar with the terms defined in [I-D.ietf-dots-requirements] [I-D.ietf-dots-use-cases]

The terminology related to YANG data modules is defined in [RFC7950]

In addition, this document uses the terms defined below:

dots svr: abbreviation of dots server.

ISP: Internet service provider.

3. DOTS server Considerations

When take dots server deployment into consideration, one thing must be involved is mitigator.so far, how many network devices can play the role of mitigator, we make a summerized list as follows:

- Router.

- Special cleaning equipment, such as Flow clean device and clean center.

- Network security equipment, such as firewall,IPS and WAF

Whether DOTS server can be deployed, the following conditions need to be met:

- DOTS server has to interconnected with mitigator

- DOTS server can go directly to the mitigator which had best go through without any other DOTS agents

- DOTS server has the permissions for scheduling and operations on mitigator

- DOTS server has the ability to know the address of attack target belong to which mitigator

4. DOTS server deployment inside an ISP

From the internal structure of ISP, the whole network can divide into three parts logically. There are three most important routers: backbone router, man(metropolitan area network) router, and IDC router. When a ddos attack occurs, it must be one of the three cases as follows, and the corresponding mitigator will responsible for mitigation.

- only the lan network detected the attack, dots server3 will receive mitigation request, and mitigator3 will act as the first responsible mitigator.

- only the man network detected the attack, dots server2 will receive mitigation request, then mitigator2 will act as the first responsible mitigator.

- only the backbone network detected the attack, dots server1 will receive mitigation request, then mitigator1 will act as the first responsible mitigator.

- Attacks on the same attack target are found both in adjacent areas, the upper network mitigator will act as the first responsible mitigator. for example, dots server1 and dots server2 both received the mitigation request from attack target by dots client, mitigator1 will responsible for ddos disposition(priority ranking: mitigator1 > mitigator2 > mitigator3).

```
                                   +---------+
                                   |other ISP|
                                   +---------+
                           .........|..........................
                                    |         backbone network
                    +---------------+     +----------+
                    |backbone router|-----|mitigator1|
                    +---------------+     +----------+
                       |dots svr1|
                       +---------+
                  ..........|.................................
                            |       metropolitan area network
                      +----------+       +----------+
                      |man router|-------|mitigator2|
                      +----------+       +----------+
                       |dots svr2|
                       +---------+
                  ..........|.........................
                            |       local area network
                      +----------+      +----------+
                      |IDC router|------|mitigator3|
                      +----------+      +----------+
                       |dots svr3|
                       +---------+
                            |
                            |
                      +-----------+       +-------------+
                      |dots client|-------|attack target|
                      +-----------+       +-------------+
```

Figure 1: DOTS Server Deployment

5. DOTS server deployment between ISPs

The coexistence of different operators is very common, coordination between operators across networks is very important. Interdomain attacks occur frequently, We recommend deploying the DOTS server at the access point

o DDoS attack from one of other ISPs, for example, ISP A received DDoS attack from ISP B or ISP C, then dots server C or dots server B will receive the mitigation request.

o DDOS attack from two or more of other ISPs,for example, ISP A and ISP B both start ddos attack to ISP C, then dots server A and dots server B will both receive mitigation request from dots client C.

```
    +-------------+        +-------------+
    |    ISP A    |--------|    ISP B    |
    | +---------+ |        | +---------+ |
    | |dots svrA| |        | |dots svrB| |
    +-------------+        +-------------+
        |                           |
        +-------------+-------------+
          |
   +-------------+
   |    ISP C    |
   | +---------+ |
   | |dots svrC| |
   +-------------+
```

Figure 2: DOTS Server Deployment2

6. Security Considerations

TBD

7. IANA Considerations

TBD

8. Acknowledgement

TBD

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

9.2. Informative References

[I-D.ietf-dots-architecture]
Mortensen, A., K, R., Andreasen, F., Teague, N., and R. Compton, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Architecture", draft-ietf-dots-architecture-14 (work in progress), May 2019.

[I-D.ietf-dots-multihoming]
Boucadair, M. and R. K, "Multi-homing Deployment Considerations for Distributed-Denial-of-Service Open Threat Signaling (DOTS)", draft-ietf-dots-multihoming-01 (work in progress), January 2019.

[I-D.ietf-dots-requirements]
Mortensen, A., K, R., and R. Moskowitz, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-22 (work in progress), March 2019.

[I-D.ietf-dots-server-discovery]
Boucadair, M. and R. K, "Distributed-Denial-of-Service Open Threat Signaling (DOTS) Server Discovery", draft-ietf-dots-server-discovery-04 (work in progress), June 2019.

[I-D.ietf-dots-signal-channel]
K, R., Boucadair, M., Patil, P., Mortensen, A., and N. Teague, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", draft-ietf-dots-signal-channel-34 (work in progress), May 2019.

[I-D.ietf-dots-use-cases]
Dobbins, R., Migault, D., Fouant, S., Moskowitz, R., Teague, N., Xia, L., and K. Nishizuka, "Use cases for DDoS Open Threat Signaling", draft-ietf-dots-use-cases-17 (work in progress), January 2019.

Authors' Addresses

Meiling Chen
CMCC
32, Xuanwumen West
BeiJing , BeiJing   100053
China

Email: chenmeiling@chinamobile.com

Li Su
CMCC
32, Xuanwumen West
BeiJing   100053
China

Email: suli@chinamobile.com

Jin Peng
CMCC
32, Xuanwumen West
BeiJing   100053
China

Email: pengjin@chinamobile.com