DOTS
Internet-Draft
Intended status: Standards Track
Expires: February 23, 2020

M. Chen
Li. Su
Jin. Peng
CMCC

August 22, 2019

DOTS client carry ddos attack informations in signal channel
draft-chen-dots-attack-informations-03

Abstract

This document describes DDoS attack information which can be obtained by DOTS client when the enterprise suspects it is under DDoS attack, these informations will be send from DOTS client to DOTS server in mitigation request using Signal channel or Data channel.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Distributed Denial of Service (DDoS) is a type of resource-consuming attack, which exploits a large number of attack resources and uses standard protocols to attack target objects. DDoS attacks consume a large amount of target network resources or server resources (including computing power, storage capacity, etc.), this means there are two types of the DDoS attack, one is bandwidth consuming attack, the other is host resource consuming attack. At present, DDoS attack is one of the most powerful and indefensible attacks on the Internet, and due to the extensive use of mobile devices and IoT devices in recent years, it is easier for DDoS attackers to attack with real attack sources (broilers).

The IETF is specifying the DDoS Open Threat Signaling (DOTS) [I-D.ietf-dots-architecture]architecture, where a DOTS client can inform a DOTS server that the attack target is under a potential attack and that appropriate mitigation actions are required. In the architecture draft, it says in the draft the enterprise has a DOTS client, which obtains information about the DDoS attack, and signals the DOTS server for help in mitigating the attack. but it doesn't says what the information of DDoS attack is. the scope of this draft is about the information of DDoS attack which DOTS client can obtain.

In the architecture draft, it says in the draft the client signal may also include telemetry information about the attack, if the DOTS client has such information available. But in the signal channel draft it doesn't define optional parameter about the telemetry information which will be regarded as DDoS portrait information.

"DDoS portrait information" is defined as the collection of attributes characterizing the attacks(or suspected attack) that have been detected and mitigated. The DDoS portrait information is an

optional set of attributes that can be signaled. The portrait can be optionally sent from the DOTS Client to Server and vice versa.

This document will divide into two directions, before mitigation request and after mitigation is complete. Before mitigation request, DOTS client can obtain informations of attack; After mitigation, DOTS server can obtain from mitigator.

2. Terminology

2.1. Key Words

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]

2.2. Definition of Terms

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:

Bandwidth consuming attack DDoS attack that causes network congestion.

Host resources consuming attack DDoS attack that consuming the ability of the protocol stack to process resources, or make host engaged in high-consumption business, thus unable to respond to normal business

Attack-bandwidth: the amount of traffic under attack, it is usually expressed numerically.

Flow clean: one selection of Attack traffic deposition, the operation contains recognize, discard and reinage.

Attack Type: used to distinguish between different methods of ddos attack.

Attack type definition: General definition method, Covers most current attack types.

Attack-source-ip-number: Number of all attack sources(ip).

Target-attack-type-threshold: The DDoS detection device sets a threshold for each type of attack, this threshold is usually exceeded to generate DDoS alarms.

3. Alarm attributes for mitigation request

3.1. Bandwidth consuming attack

3.1.1. Attack_Target_IP

The IP address of attack target, which can be either IPv4 or IPv6, supports address block notation. For example, if a company's IP address is attacked, it can aggregate IP addresses.

3.1.2. Alarm_Begin_time

If the alarm is confirmed to be real and effective after mitigation, the alarm start time is the same as the attack start time.

3.1.3. Direction

The direction of the attack, divided into inward and outward, 0 means inward, 1 means outward. Inward means attack target suffers DDoS attack, outward means attack target is launching DDoS attack.

3.1.4. Target_Attack_Type

A list of attack types involved in an attack.

3.1.5. Target_Attack_Type_Threshold

The alarm threshold set for each attack type, measurement unit can be pps or bps.

3.1.6. Attack_Target_IP_Peak

Peak of attack traffic, measurement unit can be pps or bps. We use peak of attack traffic rather than averages because peak of attack is more indicative of attacks.

3.1.7. Attack_Source_IP_Num

The number of attack source ip, measure the number of attacker's is much more helpful for the scale of attack for Bandwidth consuming attack.

3.1.8. Attack_Bandwidth

The proportion of the current traffic bandwidth to the total bandwidth of the pipeline. The attack bandwidth is described in terms of percentage. The total bandwidth is preset in the attack target.

3.2. Host resource consuming attack

3.2.1. Attack_Target_IP

The IP address of attack target, which can be either IPv4 or IPv6, supports address block notation. For example, if a company's IP address is attacked, it can aggregate IP addresses.

3.2.2. Attack_Target_Packet_Rate

All packet rates for the same protocol and the same attack target in one period. for example, A is suffering CC attack, then attack_target_packet_rate is used to calculate the number of all HTTP packets in 5 minites.

3.2.3. Alarm_Begin_Time

If the alarm is confirmed to be real and effective after mitigation, the alarm start time is the same as the attack start time.

3.2.4. Direction

The direction of the attack, divided into inward and outward, 0 means inward, 1 means outward. Inward means attack target suffers DDoS attack, outward means attack target is launching DDoS attack.

3.2.5. Target_Attack_Type

A list of attack types involved in an attack.

4. mitigation attributes for mitigation response

4.1. Bandwidth consuming attack

4.1.1. Attack_Target_IP

The IP address of attack target, which can be either IPv4 or IPv6, supports address block notation. For example, if a company's IP address is attacked, it can aggregate IP addresses.

4.1.2. Alarm_End_time

The end time of mitigation, denoted by -1 if the remission is not finished temporarily

4.1.3. Target_Attack_Type

A list of attack types involved in an attack.

4.1.4. Total_Traffic

Total traffic received by the attack target, measurement unit can be pps or bps.

4.1.5. Residual_Traffic

Residual traffic can also be considered normal business traffic, In the actual cleaning operation, that is the normal service flow injected into the link.

4.1.6. Attack_Traffic

The total attack traffic, It can be calculated by the Total_Traffic minus the Residual_Traffic

4.1.7. Attack_Target_IP_Peak

Peak of attack traffic, measurement unit can be pps or bps. After mitigation, the Attack_Target_IP_peak will be more precise for measurement.

4.1.8. Attack_Source_IP_Num

The number of attackers in the case of this whole attack.

4.2. Host resource consuming attack

4.2.1. Attack_Target_IP

The IP address of attack target, which can be either IPv4 or IPv6, supports address block notation. For example, if a company's IP address is attacked, it can aggregate IP addresses.

4.2.2. Alarm_End_time

The end time of mitigation, denoted by -1 if the remission is not finished temporarily

4.2.3. Target_Attack_Type

A list of attack types involved in an attack.

4.2.4. Attack_Source_IP

All the attack IP addresses involved in an attack.

4.2.5. Attack_Target_Packet_Rate

All packet rates for the same protocol and the same attack target in one period. for example, A is suffering CC attack, then attack_target_packet_rate is used to calculate the number of all HTTP packets in 5 minites.

5. Mitigation Use Case 1

5.1. Mitigations for attack flow

when attack target is under attack, it has to make corresponding disposal, there are two options for disposal, one is blackhole directly which may be take effect in routers, in this way all the attack flow will be discarded by router upper path of attack target, this means that the attack target will not receive any traffic during the attack depending on the routing strategy, all the traffic forwards attack target will be discarded, this has a huge impact on the work environment, especially the host that provide external service. The other way of the disposition is to drainage all the traffic flow to clean center from router, then the clean center will use pattern matching or any other method to find out the attack traffic flow to discard, finally, clean center reinage the normal business traffic back to attack target by upper router, the whole process above is defined as flow clean(Figure 1).

```
attack flow +--------+                  +--------+
----------->| router |----------------->| clean  |
  1         +--------+        2         | center |
             |                          +--------+
           3 |                              |
             |       +--------+             |
             +------>| attack |<------------+
                     | target |
                     +--------+
```

Figure 1: diagram of DDoS Mitigation usecase

Generally, the bandwidth of the link 1 must be larger than link 2 and link 3, and the clean ability of clean center limited to hardware resources. An example of link situation is as below(Figure 2):

figure tag	bandwidth/ capability
link 1	100Gb
link 2	50Gb
link 3	10Gb
clean center	80Gb

Figure 2: an example of link bandwidth

The Figure2 is a scenario of the link bandwidth, when a ddos attack is ongoing, if the link 1 bandwidth is completely jammed, the best way to mitigate the attack is to discard all the attack flow; if the amount of the traffic flow is lower than the remainder cleaning ability, the most suitable disposition is to drainage all the attack flow to clean center. Therefore, it is an obvious requirement in the current network environment.

5.2. Optimal device selection

Mitigator may owns a cleaning device cluster and can manage cleaning devices. The capacity of each cleaning equipment is variable, usually each cleaning equipment utilization rate is different, then the remaining cleaning capacity is not consistent. When the attack flow is less than the ability of a cleaning equipment, according to the attack-bandwidth can choose a suitable cleaning equipment, that is conducive to the utilization of equipment; When the attack flow is larger than the cleaning capacity of one cleaning device, several cleaning devices can be optimally scheduled according to the attack-bandwidth.

5.3. Optimum path for disposal

When mitigator is an attack flow cleaning service, they typically deployed the mitigator in a distributed way because of the cost of bandwidth usage with their own leased operator's link bandwidth, and choosing the best traction path was the key to profitability. If the parameter of attack-bandwidth is carried, then the generation of the best drainage path is very meaningful.

When mitigator is at the upstream service operator level, they might have multiple networks, with the attack alert using one network and the flow drainage using another, and the link load is not the same, then carrying the attack-bandwidth is very beneficial for choosing the drainage path, mainly for link load balancing.

5.4. Mitigation request parameters

When a DOTS client requires mitigation for some reason, the DOTS client uses the CoAP PUT method to send a mitigation request to its DOTS server(s). If a DOTS client is entitled to solicit the DOTS service, the DOTS server enables mitigation on behalf of the DOTS client by communicating the DOTS client's request to a mitigator (which may be colocated with the DOTS server) and relaying the feedback of the thus-selected mitigator to the requesting DOTS client.

DOTS clients use the PUT method to request mitigation from a DOTS server. During active mitigation, DOTS clients may use PUT requests to carry mitigation efficacy updates to the DOTS server. We suggest to add attack bandwidth to satiesfy the requirement.

total traffic when ddos attack occur, reflects the urgency of the current attack. Serious attacks are treated with blackhole, Other cases use flow cleaning, attack-bandwidth is conducive to the selection of disposal mode.

This is an optional attribute.

6. Mitigation Use Case 2

6.1. classified disposal

DDoS attack is a hybrid attack across multiple protocol layers and multiple method, when we deal with DDoS attacks, we find it more reasonable and effective to deal with them according to the types of attacks, It is easier to handle if the type of attack is already included in the mitigation request. There is no doubt that the information may not be accurate, but we can take it as a reference. Therefore, with attack type the disposal process is more helpful. The ddos attack alarm in the industry is set according to the attack type, from the point of view of cleaning, different types of attacks are handled differently. For example, Memcached reflection flood use UDP 11211 port for DDoS flood, but tcp syn flood use defects of TCP three-way handshake to consuming connection resources. This two attacks are alarmed respectively and cleaned in different ways. We suggest to add attack type to satiesfy the requirement.

A list of attack types involved in an attack.

There is no uniform definition of attack types, It is often the case that the same type of attack has different names, An attack type is defined in section 4.

The parameter of Target_Attack_Type contains three values: Attack_Name, Attack_Alias and Target_Attack_Type_Threshold, Attack_Alias will solve the abbreviation problem.An attack could be a hybrid attack, then the target_Attack_Type represents major types of attacks

This is an optional attribute.

6.2. Standard of Attack Type Definition

For the Target_Attack_Type field, we define it as a string Type, and define the two fields according to the attack method and extension name. there may be problems in the actual network environment, that attack target and mitigator (such as cleaning equipment) belong to different models of different vendors, because different vendors have different definitions of Attack in understanding and implementation. When an attack occurs, some devices may not be considered as an attack. It is also possible that the detection device considere it as A type attack, while the cleaning device consider it as B type attack. When performing the cleaning schedule, it will cause the problem of incorrect cleaning or over-cleaning. Both of these errors will cause the normal business to fail to link. Therefore, it is necessary to unify the attack definition, form a standard attack definition, and solve the problem of cleaning errors from the source. we give out a complete format for DDoS attacks as below:

[protocol layer] [protocol name] [message name/operation name/port] [attack methods feature description field 1] [attack methods feature description field 2] [attack methods describe the standard field]

protocol layer(mandatory): Network layer, transport layer, application layer;

protocol name(mandatory): The protocol type used for the attack, such as http, TCP, ICMP, NTP...;

message name/ operation name/ port(optional): The message name, operation name, or port used for the attack is a further addition to the protocol used for the attack, with message names such as SYN and operation names such as GET, Post, SYN, ACK, Query...;

attack methods feature description field 1 or 2 (optional): Description of the method used in the attack, such as Fragment, Amplification, Misuse, Slow...;

attack methods describe the standard field(mandatory): Used to describe the type of attack, as the end field, such as flood, attack;

The protocol name and message name must contain at least one item in the abbreviation.

interval between each field operators use special symbol or any other symbol agreed. For example:HTTP Get Flood(CC) definition, we defined the Target_Attack_Type field as below(Figure 3):


```
{
  "Attack_Name":" Application_Layer, HTTP, Get,,, Flood"
  "Attack_Alias":"HTTP CC Flood"
  "Target_Attack_Type_Threshold":"1000pps"

}
```


Figure 3: Attack type definition example

An example of abbreviation: Define the target-attack-type using the methods specified above, complete attack name: Transport_Layer TCP SYN Flood; abbreviated form: TCP SYN Flood.

7. Mitigation Use Case 3

7.1. Mitigation alarm baseline

Attack target looks like to be attacked by DDoS, then DOTS client send mitigation request to DOTS server, So there are exist false alarms. In practice, there are standards for alerting whether or not they are appropriate, such as alarm baseline. With this parameter, it is possible to determine whether the standard is reasonable or not, False alarms can be corrected and normal alarms can be optimized. It is suggested to use Target_Attack_Type_Threshold to carry this information.

DDoS attacks are distributed attacks, it means there are many sources of attack that the traffic from each attack source varies little, so it is more efficient to record the numbers of source ip than the details ip address. Blocking every IP address is a thankless task and short-lived. After mitigation, mitigators can feedback the source ip number to DOTS server, and this information must be more closer to the attack scene, these informations will be used in the feedback module for more application.

Target_Attack_Type_Threshold: Baseline for a type of attack .

If attack target have the ability to classify each type of DDoS attack, it must have ability to feedback criteria for each type of attack. It doesn't matter that if it can not provide this information, it is just an optional attribute.

This is an optional attribute.

8. Mitigation request optional parameters

8.1. Bandwidth consuming attack

Added parameters show in put method for Bandwidth consuming attack are show as below(Figure 4)


```
Content-Format: "application/dots+cbor"
                  {
                  "ietf-dots-signal-channel:mitigation-scope": {
                    "scope": [
                      {
                        "target-prefix": [
                           "string"
                         ],
                        "target-port-range": [
                           {
                             "lower-port": number,
                             "upper-port": number
                           }
                         ],
                         "target-protocol": [
                           number
                         ],
                         "target-fqdn": [
                           "string"
                         ],
                         "Attack_Target_IP":[
                                "string"
                         ],
                         "Alarm_Begin_time":[
                                "string"
                         ],
                         "Direction":[
                                 number
                         ],
                         "Attack_Target_IP_peak":[
                                "string"
                         ],
```

```
                          "Attack_Source_IP_Num":[
                                 "string"
                          ],
                          "Target_Attack_Type": [
                             {
                               "Attack-Name": ["string"],
                               "Attack-Alias": ["string"],
                               "Target_attack_Type_threshold":["string"]
                             }
                           ],
                           "Attack_Bandwidth":[
                                 "string"
                           ],
                           attack_src_ip_number:[
                             "string"
                           ],

                           "target-uri": [
                            "string"
                          ],
                          "alias-name": [
                            "string"
                          ],
                         "lifetime": number,
                         "trigger-mitigation": true|false
                       }
                     ]
                   }
                   }
```

Figure 4: Mitigation request for Bandwidth consuming attack

8.2. Host resource consuming attack

Added parameters show in put method for Host resource consuming attack are show as below(Figure 5)

```
    Content-Format: "application/dots+cbor"
                     {
                     "ietf-dots-signal-channel:mitigation-scope": {
                       "scope": [
                         {
                           "target-prefix": [
                              "string"
                            ],
                           "target-port-range": [
                              {
```

```
                        "lower-port": number,
                        "upper-port": number
                      }
                    ],
                    "target-protocol": [
                      number
                    ],
                    "target-fqdn": [
                      "string"
                    ],
                    "Attack_Target_IP":[
                           "string"
                    ],
                    "Alarm_Begin_time":[
                           "string"
                    ],
                    "Direction":[
                            number
                    ],
                    "Attack_Target_Packet_Rate":[
                           "string"
                    ],
                   "Target_Attack_Type": [
                       {
                         "Attack-Name": ["string"],
                         "Attack-Alias": ["string"],
                        }
                     ],
                     "target-uri": [
                      "string"
                    ],
                    "alias-name": [
                      "string"
                    ],
                   "lifetime": number,
                   "trigger-mitigation": true|false
                 }
               ]
             }
             }
```


Figure 5: Mitigation request for Host resource consuming attack

9. Mitigation response parameters

After the mitigation of a DDoS attack, DOTS server can obtain some informations from mitigator, these informations are optional parameters only as a suggestion when use DOTS to inform the message between attack target and mitigator.

9.1. Bandwidth consuming attack

added parameters of Mitigation response for Bandwidth consuming attack, Figure6Figure 6


```
  Content-Format: "application/dots+cbor"
                 {
                 "ietf-dots-signal-channel:mitigation-scope": {
                   "scope": [
                     {
                       "target-prefix": [
                          "string"
                        ],
                       "target-port-range": [
                          {
                            "lower-port": number,
                            "upper-port": number
                          }
                        ],
                        "target-protocol": [
                          number
                        ],
                        "target-fqdn": [
                          "string"
                        ],
                        "Attack_Target_IP":[
                               "string"
                        ],
                        "Alarm_End_time":[
                               "string"
                        "],
                        "Total_Traffic":[
                                "string"
                        ],
                        "Residual_Traffic":[
                               "string"
                        ],
                        "Attack_Traffic":[
                               "string"
                        ],
                        "Attack_Target_IP_Peak":[
```

```
                                "string"
                         ],
                         "Attack-Source-IP-Num":[
                                "string"
                         ],
                        "Target_Attack_Type": [
                            {
                              "Attack-Name": ["string"],
                              "Attack-Alias": ["string"],
                              "Target_attack_Type_threshold":["string"]
                            }
                          ],
                          "target-uri": [
                           "string"
                         ],
                         "alias-name": [
                           "string"
                         ],
                        "lifetime": number,
                        "trigger-mitigation": true|false
                      }
                    ]
                  }
                  }
```


Figure 6: Mitigation response for Bandwidth consuming attack

9.2. Host resource consuming attack

added parameters of Mitigation response for Bandwidth consuming attack, Figure7Figure 7


```
    Content-Format: "application/dots+cbor"
                    {
                    "ietf-dots-signal-channel:mitigation-scope": {
                      "scope": [
                        {
                          "target-prefix": [
                             "string"
                           ],
                          "target-port-range": [
                             {
                               "lower-port": number,
                               "upper-port": number
                             }
                           ],
                           "target-protocol": [
```

```
                                number
                              ],
                              "target-fqdn": [
                                "string"
                              ],
                              "Attack_Target_IP":[
                                     "string"
                              ],
                              "Alarm_End_time":[
                                     "string"
                              "],

                              "Attack_Source_IP":[
                                     "string"
                              ],
                              "Attack_Target_Packet_Rate":[
                                     "string"
                              ],
                             "Target_Attack_Type": [
                                 {
                                   "Attack-Name": ["string"],
                                   "Attack-Alias": ["string"],
                                 }
                               ],
                               "target-uri": [
                                "string"
                              ],
                              "alias-name": [
                                "string"
                              ],
                             "lifetime": number,
                             "trigger-mitigation": true|false
                           }
                         ]
                       }
                       }
```


Figure 7: Mitigation response for Host resource consuming attack

10. Security Considerations

TBD

11. IANA Considerations

TBD

12. Acknowledgement

TBD

13. References

13.1. 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>.

13.2. 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-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-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-37 (work in progress), July 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-19 (work in progress), July 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