DOTS
Internet-Draft
Intended status: Experimental
Expires: September 10, 2019

M. Chen
Li. Su
CMCC

March 9, 2019

expand attack type in signal channel
draft-meiling-dots-attack-type-expansion-00

Abstract

This document describes a DDoS Mitigation Request parameter used in the Signal Channel request, as an expansion of the signal channel for mitigating DDoS attack accurately with attack types. The proposed parameter will help to achieve fine-grained disposition for the attack traffic to be cleaned.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 10, 2019.

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 object network resources or server resources (including computing power, storage capacity, etc.) of the target object, so that the target object cannot provide network services normally. 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).

Why again raise the parameter of attack type to add to mitigation request for discussion; Although the scope of DOTS work now is the interaction between DOTS client and DOTS server, the mitigator and attack target roles must be considered in the implementation when use DOTS mechanism. It has been discussed before whether it is appropriate to carry the type of attack in the mitigation request parameters. Some views hold that the type of attack reported is not credible.The premise of this view is that both attack detection and attack disposal belong to the mitigator role. But there is another scenario in which attack detection and attack disposal are separated, and one possible scenario in which the attack detection is at the attack target and the attack disposal is at the mitigator, then attack informations such as the attack type is trusted.We can also consider a scenario, if an entity is not only the attack target, but also a mitigator, when ddos attack occurs, it requires other mitigators upper link to mitigate the attack flow, so it will use

dots client send mitigation reqest to other top link mitigator together, in this case all the mitigators can share informations of the attack, and the informations are fully trusted, in this way, other mitigator does not need to waste of resources for detecting again.

Why do we need uniform attack types. At present, telecom operators, cloud service providers and third-party manufacturers have their own anti-ddos solutions.The construction of DDoS attack mitigation and disposal system involves two devices, namely detection equipment and cleaning equipment. In the actual network deployment, the core nodes of the network will deploy detection equipment and cleaning equipment at the same time to detect and dispose attacks. After an alarm is given, the cleaning equipment will be triggered to carry out traffic drainage and cleaning operations. At present, the detection equipment adopts the coarse-grained attack type determination method, which greatly reduces the false alarm rate of attack.Different disposal of cleaning equipment is different for different attack types. For example, UDP attack types can be discarded directly after matching, but HTTP CC Flood can be further determined only after interactive operation is required at the disposal. Interactive operation may be redirection or verification code sending. In the actual environment, there are many manufacturers of detection equipment and cleaning equipment, and each manufacturer has its own definition method of attack type, so it is easy to lead to the same attack, but the field of attack type detected by different equipment manufacturers is not the same, which may easily lead to disposal confusion.

Volume based distributed denial-of-service attack have many types based on different protocol layer, for the service providers to immediately protect their network services from DDoS attacks, DDoS mitigation needs to be automated. 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. This document describe attack type in the mitigation request.

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:

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

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

3. Request Mitigation expansion

The purpose of this expansion is to propose the attack traffic more accurately. 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. AS the mitigator doesn't have to detect the attack type again, the mitigator can directly do the drainage of attack flow. Therefore, with attack type the disposal process is more efficient.

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 cleaned in different ways. Therefore, it is necessary to add attack type parameters in the mitigation request.

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.

The two new parameters in the CBOR body (Figure 1) are described below:


```
 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"
                        ],
                        "target-Attack-Type": [
                           {
```

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

Figure 1: PUT to Convey DOTS Mitigation Requests

target-attack-type: 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 two value, one is Attack-Name, the other is Attack-Alias, 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.

The definition of the rest parameters are the same as the [I-D.ietf-dots-signal-channel]

4. 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 level] [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]

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:

```
{
  "Attack-Name":" Application _Layer, HTTP, Get,,, Flood"
  "Attack-Alias":"HTTP CC Flood"

}
```

Figure 2: Attack type definition example

Based on the extension, the DOTS Server can accurately inform Mitigator of the objects and attack types that need to be disposed when the mitigation instructions are delivered to the Mitigation, so that the Mitigator can be accurately disposed.

5. Security Considerations

TBD

6. IANA Considerations

TBD

7. Acknowledgement

TBD

8. References

8.1. 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>.

8.2. Informative References

[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-20 (work in progress), February 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-30 (work in progress), March 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