DOTS
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2019

T. Reddy
J. Harsha
McAfee
M. Boucadair
Orange
J. Shallow
NCC Group

October 16, 2018

Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Call Home

draft-reddy-dots-home-network-00

Abstract

This document presents DOTS signal channel Call Home service, which enables a DOTS server to initiate a secure connection to a DOTS client, and to receive the attack traffic information from the DOTS client. The DOTS server in turn uses the attack traffic information to identify the compromised devices launching the outgoing DDOS attack and takes appropriate mitigation action.

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 April 19, 2019.

Table of Contents

1. Introduction

1.1. The Problem

The DOTS signal channel protocol [I-D.ietf-dots-signal-channel] is used to carry information about a network resource or a network (or a part thereof) that is under a Distributed Denial of Service (DDoS) attack. Such information is sent by a DOTS client to one or multiple DOTS servers so that appropriate mitigation actions are undertaken on traffic deemed suspicious. Various use cases are discussed in [I-D.ietf-dots-use-cases].

IoT devices are becoming more and more prevalent in home networks, and with compute and memory becoming cheaper and cheaper, various types of IoT devices are available in the consumer market at affordable price. But on the downside, the main threat being most of these IoT devices are bought off-the-shelf and most manufacturers haven't considered security in the product design. IoT devices deployed in home networks can be easily compromised, they do not have easy mechanism to upgrade, and IoT manufactures may cease manufacture

and/or discontinue patching vulnerabilities on IoT devices. However, these vulnerable and compromised devices will continue be used for a long period of time in the home, and the end-user does not know that IoT devices in his/her home are compromised. The compromised IoT devices are typically used for launching DDoS attacks on the victim while the owner/administrator of the home network is not aware about such misbehaviors. Similar to other DDoS attack, the victim in this attack can be an application server, a host, a router, a firewall, or an entire network.

Nowadays, network devices in a home network offer network security, for instance, firewall/IPS service on a home router or gateway to protect the devices connected to the home network from external and internal attacks. Over the years several techniques have been identified to detect DDoS attacks, some of these techniques can be enabled on home network devices but most of them are used in the Internet Service Provider (ISP)'s network. The ISP offering DDoS mitigation service can detect outgoing DDoS attack traffic originating from its subscribers or the ISP may receive filtering rules (for example, using BGP flowspec [RFC5575]) from downstream service provider to filter, block, or rate-limit DDoS attack traffic originating from the ISP's subscribers to the downstream target.

Some of the DDoS attacks like spoofed RST or FIN packets, Slowloris, and TLS re-negotiation are difficult to detect on the home network devices without adversely affecting its performance. The reason is typically home routers have fast path to boost the throughput. For every new TCP/UDP flow, only the first few packets are punted through the slow path. Hence, it is not possible to detect various DDoS attacks in the slow path, since the attack payload is sent to the target server after the flow is switched to fast path. Deep packet inspection (DPI) of all the packets of a flow would be able to detect some of the attacks. However, a full-fledged DPI to detect these type of DDoS attacks is functionally or operationally not possible for all the devices attached to the home network owing to the memory and CPU limitations of the home routers. Further, for certain DDoS attacks the ability to distinguish legitimate traffic from attacker traffic on a per packet basis is complex. This complexity originates from the fact that the packet itself may look "legitimate" and no attack signature can be identified. The anomaly can be identified only after detailed statistical analysis.

The ISP on the other hand can detect the DDoS attack originating from a home network, but the ISP does not have a mechanism to detect which device in the home network is generating the DDoS attack traffic. The primary reason being that devices in a IPv4 Home network are typically behind a NAT border. Even in case of a IPv6 Home network, although the ISP can identify the infected device in the Home network

launching the DDoS traffic by tracking its unique IPv6 address, the infected device can easily change the IP address to evade remediation.

Existing approaches are still suffering from misused access network resources by abusing devices; the support of means for blocking such attacks close to the sources are missing. In particular, the DOTS signal protocol do not discuss cooperative DDoS mitigation between the home network and ISP to the suppress the outbound DDoS attack traffic originating from the home network.

1.2. The Solution

This specification addresses the problems discussed in Section 1.1 and presents DOTS signal channel Call Home extension, which enables the DOTS server to initiate a secure connection to the DOTS client, and the DOTS client then conveys the attack traffic information to the DOTS server. The DOTS server uses the DDoS attack traffic information to identify the compromised device in its domain launching the DDoS attack, notifies the network administrator, and takes appropriate mitigation action. The mitigation action can be to quarantine the compromised device or block its traffic to the attack target until the mitigation request is withdrawn.

For instance, the DOTS server in the home network initiates the Call Home during peace time and then subsequently the DOTS client in the ISP environment can initiate mitigation requests whenever the ISP detects there is an attack from a compromised device in the DOTS server's domain.

2. Notational Conventions and 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 BCP 14 [RFC2119][RFC8174] when, and only when, they appear in all capitals, as shown here.

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

3. DOTS Signal Channel Call Home

3.1. Procedure

DOTS signal channel Call Home preserves all but one of the DOTS client/server roles in the DOTS protocol stack, as compared to DOTS client-initiated DOTS signal channel protocol. The one and only role

reversal that occurs are at the TCP/TLS or DTLS layers; that is, the DOTS server acts as a DTLS client and the DOTS client acts as a DTLS server or the DOTS server acts as a TCP/TLS client and the DOTS client acts as a TCP/TLS server. The DOTS server initiates TCP/TLS handshake or DTLS handshake to the DOTS client.

For example, a home network element (e.g., home router) co-located with a DOTS server (likely, a client-domain DOTS gateway) is the TCP/TLS server and DTLS server. However, when calling home, the DOTS server initially assumes the role of the TCP/TLS client and DTLS client, but the network element's role as a DOTS server remains the same. Further, existing certificate chains and mutual authentication mechanisms between the DOTS agents are unaffected by Call Home function. This Call Home function enables the DOTS server co-located with a network element (possibly behind NATs and firewalls) reachable by only the intended DOTS client and hence the DOTS server cannot be subjected to DDoS attacks. Other motivations for introducing Call Home are discussed in Section 1.1 of [RFC8071].

Figure 1 illustrates sample Call Home flow exchange:

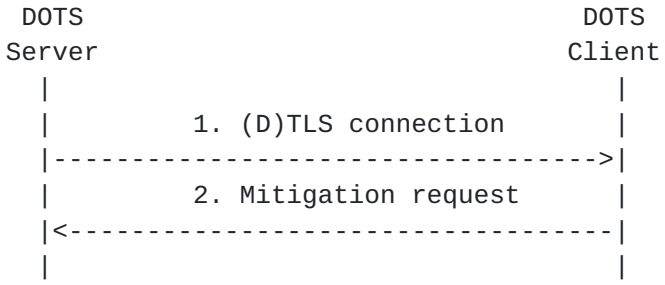

Figure 1: DOTS Signal Channel Call Home Sequence Diagram

This diagram makes the following points:

1. If UDP transport is used, the DOTS server begins by initiating a DTLS connection to the DOTS client. The DOTS client MUST support accepting DTLS connection on the IANA-assigned port defined in Section 4.1, but MAY be configured to listen to a different port. If TCP is used, the DOTS server begins by initiating a TCP connection to the DOTS client. The DOTS client MUST support accepting TCP connections on the IANA-assigned port defined in Section 4.1, but MAY be configured to listen to a different port. Using this TCP connection, the DOTS server initiates an TLS connection to the DOTS client. The happy eyeballs mechanism explained in Section 4.3 of [I-D.ietf-dots-signal-channel] can be used for initiation of both TCP and UDP sessions.

2. Using this (D)TLS connection, the DOTS client requests, withdraws, or retrieves the status of mitigation requests.

3.2. DOTS Signal Channel Extension

3.2.1. Mitigation Request

This specification extends the mitigation request defined in [I-D.ietf-dots-signal-channel] to convey the attacker source prefixes and source port numbers. The DOTS client in the mitigation request conveys the following new parameters in the CBOR body of the mitigation request:

source-prefix: A list of attacker prefixes used to attack the target. Prefixes are represented using Classless Inter-Domain Routing (CIDR) notation [RFC4632].
As a reminder, the prefix length MUST be less than or equal to 32 (resp. 128) for IPv4 (resp. IPv6).

The prefix list MUST NOT include broadcast, loopback, or multicast addresses. These addresses are considered as invalid values. In addition, the DOTS client MUST validate that attacker prefixes are within the scope of the DOTS server's domain.

This is an optional attribute.

source-port-range: A list of port numbers used by the attack traffic flows.

A port range is defined by two bounds, a lower port number (lower-port) and an upper port number (upper-port). When only 'lower-port' is present, it represents a single port number.

For TCP, UDP, Stream Control Transmission Protocol (SCTP) [RFC4960], or Datagram Congestion Control Protocol (DCCP) [RFC4340], a range of ports can be, for example, 0-1023, 1024-65535, or 1024-49151.

This is an optional attribute.

source-icmp-type: A list of ICMP types used by the attack traffic flows. A ICMP type range is defined by two bounds, a lower ICMP type number (lower-type) and an upper ICMP type number (upper-type). When only 'lower-type' is present, it represents a single ICMP type number. This is an optional attribute.

This is an optional attribute.

The 'source-prefix' and 'target-prefix' parameters are mandatory attributes when the attack traffic information is signaled by the DOTS client. The 'target-uri' or 'target-fqdn' parameters can be included in the mitigation request for diagnostic purpose to notify the DOTS server domain administrator but SHOULD not be used to determine the target IP addresses.

The DOTS server uses the attack traffic information to find the pre-NAT source IP address of the compromised device and blocks the traffic from the compromised device traffic to the attack target until the mitigation request is withdrawn. The DOTS server domain administrator consent MAY be required to block the traffic from the compromised device to the attack target. An implementation MAY have a configuration knob to block the traffic from the compromised device to the attack target with or without DOTS server domain administrator consent. If the attack traffic is blocked, the DOTS server informs the DOTS client that the attack is being mitigated.

If the attack traffic information is identified by the DOTS server or the DOTS server domain administrator as legitimate traffic, the mitigation request is rejected, and 4.09 (Conflict) is returned to the DOTS client. The conflict-clause (defined in Section 4.4.1 of [I-D.ietf-dots-signal-channel]) indicates the cause of the conflict. The following new value is defined:

4: Mitigation request rejected. This code is returned by the DOTS server to indicate the attack traffic has been classified as legitimate traffic.

If the DOTS server is co-located with a home router, it can program the packet processor to punt all the traffic from the compromised device to the target to slow path. The home router inspects the punted slow path traffic to detect and block the outgoing DDoS attack traffic or quarantine the device (e.g., using MAC level filtering) until it is remediated, and notifies the home administrator about the compromised device.

TBD:

a) Do we also want to convey Attack Name/type or ID (the home router may not be capable of detecting new emerging/sophisticated attacks) ?

b) Is DOTS data channel Call Home service required (if required, can RESTCONF Call Home defined in RFC8071 be used) ?

3.2.2. DOTS Signal Call Home YANG Module

3.2.2.1. Mitigation Request Tree Structure

This document augments the "dots-signal-channel" DOTS signal YANG module defined in [I-D.ietf-dots-signal-channel] for signaling the attack traffic information. This document defines the YANG module "ietf-dots-signal-call-home", which has the following structure:

```
module: ietf-dots-signal-call-home
  augment /ietf-signal:dots-signal:
    +--rw source-prefix*       inet:ip-prefix
    +--rw source-port-range* [lower-port upper-port]
       +--rw lower-port    inet:port-number
       +--rw upper-port    inet:port-number
    +--rw source-icmp-type-range* [lower-type upper-type]
       +--rw lower-type    uint8
       +--rw upper-type    uint8
```

3.2.2.2. Call Home Mitigation Request YANG Module

```
<CODE BEGINS> file "ietf-dots-signal-call-home@2018-09-28.yang"

module ietf-dots-signal-call-home {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-dots-signal-call-home";
  prefix signal-call-home;

  import ietf-inet-types {
    prefix inet;
    reference
      "Section 4 of RFC 6991";
  }
  import ietf-dots-signal-channel {
    prefix ietf-signal;
    reference
      "RFC XXXX: Distributed Denial-of-Service Open Threat
                 Signaling (DOTS) Signal Channel Specification";
  }

  organization
    "IETF DDoS Open Threat Signaling (DOTS) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/dots/>
     WG List:  <mailto:dots@ietf.org>

     Editor:  Konda, Tirumaleswar Reddy
              <mailto:TirumaleswarReddy_Konda@McAfee.com>;
```

```
        Editor:  Mohamed Boucadair
                 <mailto:mohamed.boucadair@orange.com>;

        Editor:  Jon Shallow
                    <mailto:jon.shallow@nccgroup.com>";

     description
       "This module contains YANG definition for the signaling
        messages exchanged between a DOTS client and a DOTS server.

        Copyright (c) 2018 IETF Trust and the persons identified as
        authors of the code.  All rights reserved.

        Redistribution and use in source and binary forms, with or
        without modification, is permitted pursuant to, and subject
        to the license terms contained in, the Simplified BSD License
        set forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (http://trustee.ietf.org/license-info).

        This version of this YANG module is part of RFC XXXX; see
        the RFC itself for full legal notices.";

     revision 2018-09-28 {
       description
         "Initial revision.";
       reference
         "RFC XXXX: Distributed Denial-of-Service Open Threat
                    Signaling (DOTS) Signal Channel Call Home";
     }

     augment "/ietf-signal:dots-signal" {
       when "message-type='mitigation-scope'";
       description "Attacker source details";

       leaf-list source-prefix {
         type inet:ip-prefix;
         description
           "IPv4 or IPv6 prefix identifying the attacker(s).";
       }
       list source-port-range {
         key "lower-port upper-port";
         description
           "Port range. When only lower-port is
            present, it represents a single port number.";
         leaf lower-port {
           type inet:port-number;
           mandatory true;
```

```
          description
            "Lower port number of the port range.";
        }
        leaf upper-port {
          type inet:port-number;
          must ". >= ../lower-port" {
             error-message
               "The upper port number must be greater than
                or equal to lower port number.";
          }
          description
            "Upper port number of the port range.";
        }
      }
      list source-icmp-type-range {
        key "lower-type upper-type";
        description
          "ICMP type range. When only lower-type is
           present, it represents a single ICMP type number.";
        leaf lower-type {
          type uint8;
          mandatory true;
          description
            "Lower ICMP type number of the ICMP type range.";
        }
        leaf upper-type {
          type uint8;
          must ". >= ../lower-type" {
             error-message
               "The upper ICMP type number must be greater than
               or equal to lower ICMP type number.";
          }
          description
            "Upper type number of the ICMP type range.";
        }
      }
    }
  }
```

4. IANA Considerations

4.1. DOTS Signal Channel Call Home UDP and TCP Port Number

IANA is requested to assign the port number TBD to the DOTS signal channel Call Home protocol for both UDP and TCP from the "Service Name and Transport Protocol Port Number Registry" available at: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

The assignment of port number 4647 is strongly suggested (DOTS signal channel uses port number 4646).

4.2. DOTS Signal Channel CBOR Mappings Registry

This specification registers the 'source-prefix' and 'source-port-range' parameters in the IANA "DOTS Signal Channel CBOR Mappings" registry established by [I-D.ietf-dots-signal-channel].

The source-prefix and source-port-range are comprehension-optional parameters.

Parameter Name	YANG Type	CBOR Key	CBOR Major Type & Information	JSON Type
source-prefix	leaf-list inet: ip-prefix	0x8000 (TBD)	4 array 3 text string	Array String
source-port-range	list	0x8001 (TBD)	4 array	Array
source-icmp-type-range	list	0x8002 (TBD)	4 array	Array
lower-type	uint8	0x8003 (TBD)	0 unsigned	Number
upper-type	uint8	0x8004 (TBD)	0 unsigned	Number

Table 4: CBOR Mappings Used in DOTS Signal Channel Messages

4.3. DOTS Signal Channel YANG Module

This document requests IANA to register the following URIs in the "IETF XML Registry" [RFC3688]:

```
URI: urn:ietf:params:xml:ns:yang:ietf-dots-signal-call-home
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.
```

This document requests IANA to register the following YANG modules in the "YANG Module Names" registry [RFC7950].

```
name: ietf-signal-call-home
namespace: urn:ietf:params:xml:ns:yang:ietf-dots-signal-call-home
prefix: signal-call-home
reference: RFC XXXX
```

5. Security Considerations

This document deviates from standard DOTS signal channel usage by having the DOTS server initiate the TCP/TLS or DTLS connection. DOTS signal channel related security considerations discussed in Section 10 of [I-D.ietf-dots-signal-channel] MUST be considered. DOTS agents MUST authenticate each other using (D)TLS before a DOTS signal channel session is considered valid.

An attacker may launch a DoS attack on the DOTS client by having it perform computationally expensive operations, before deducing that the attacker doesn't possess a valid key. For instance, in TLS 1.3 [RFC8446], the ServerHello message contains a Key Share value based on an expensive asymmetric key operation for key establishment. Common precautions mitigating DoS attacks are recommended, such as temporarily blacklisting the source address after a set number of unsuccessful authentication attempts.

6. Acknowledgements

TBC.

7. References

7.1. Normative References

[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-25 (work in progress), September 2018.

[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>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

7.2. Informative References

[I-D.ietf-dots-requirements]
Mortensen, A., Moskowitz, R., and R. K, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", draft-ietf-dots-requirements-15 (work in progress), August 2018.

[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-16 (work in progress), July 2018.

[RFC4340] Kohler, E., Handley, M., and S. Floyd, "Datagram Congestion Control Protocol (DCCP)", RFC 4340, DOI 10.17487/RFC4340, March 2006, <https://www.rfc-editor.org/info/rfc4340>.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006, <https://www.rfc-editor.org/info/rfc4632>.

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, DOI 10.17487/RFC4732, December 2006, <https://www.rfc-editor.org/info/rfc4732>.

[RFC4960] Stewart, R., Ed., "Stream Control Transmission Protocol", RFC 4960, DOI 10.17487/RFC4960, September 2007, <https://www.rfc-editor.org/info/rfc4960>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <https://www.rfc-editor.org/info/rfc5575>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC8071] Watsen, K., "NETCONF Call Home and RESTCONF Call Home", RFC 8071, DOI 10.17487/RFC8071, February 2017, <https://www.rfc-editor.org/info/rfc8071>.

Authors' Addresses

Tirumaleswar Reddy
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: kondtir@gmail.com

Joshi Harsha
McAfee, Inc.
Embassy Golf Link Business Park
Bangalore, Karnataka 560071
India

Email: harsha_joshi@mcafee.com

Mohamed Boucadair
Orange
Rennes 35000
France

Email: mohamed.boucadair@orange.com

Jon Shallow
NCC Group
UK

Email: supjps-ietf@jpshallow.com