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

https://tools.ietf.org/html/draft-reddy-dots-home-network-03

IETF 104, Prague

March 2019

Presenter: T. Reddy (McAfee)

J.Harsha (McAfee)

M. Boucadair (Orange)

J. Shallow (NCC)

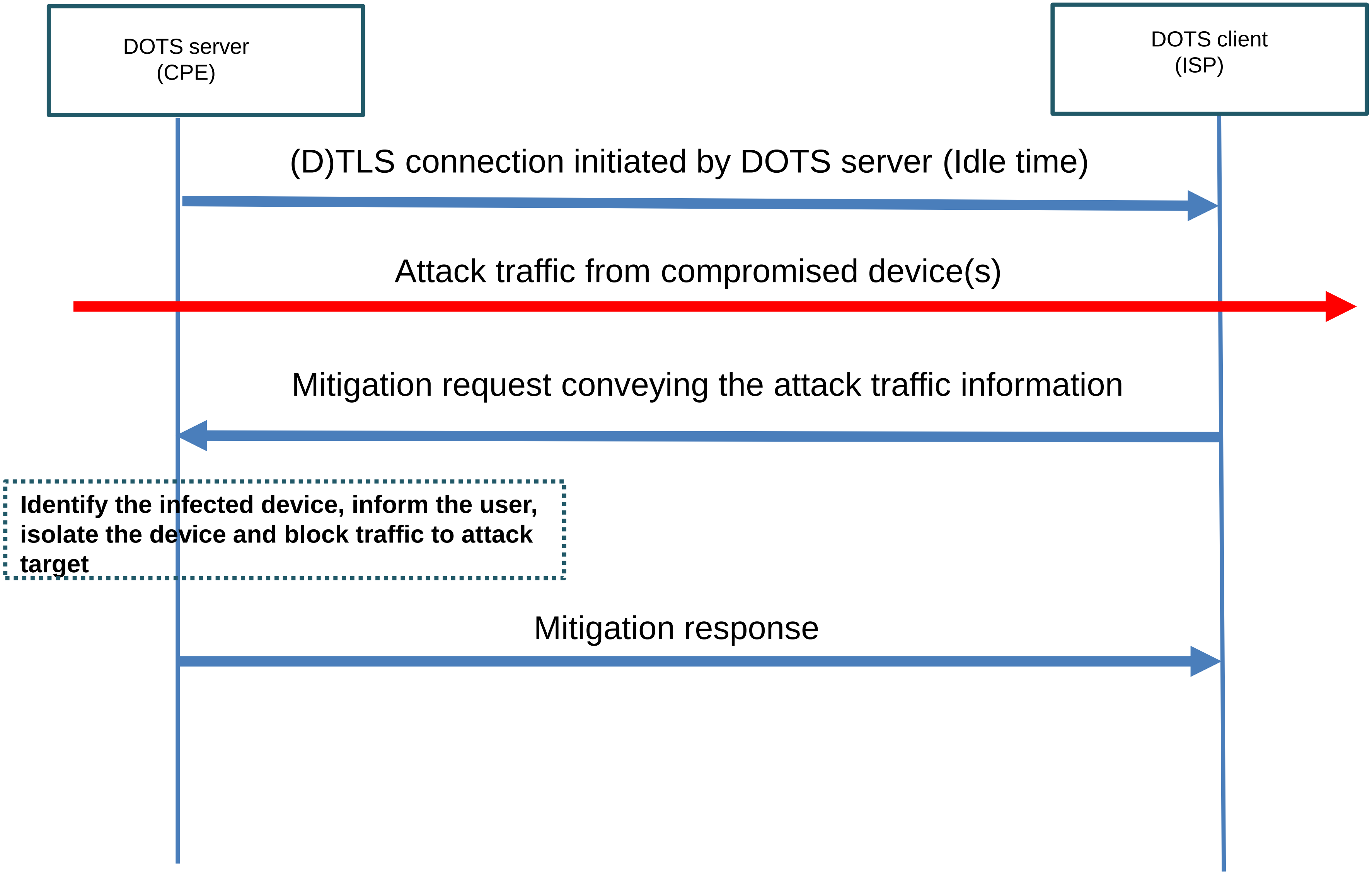
Agenda

- Problem Statement
- Solution Overview
- Updates to the draft
- Questions & Comments

Problem Statement

- ISP can detect DDoS traffic from the home network but cannot identify infected devices (behind NAT) in the home network
    - ISP cannot quarantine/isolate the infected device
    - Some heuristic to detect attacks may not be deterministic (e.g., flash crowds)
    - Rate-limiting or blocking the traffic from Home network can result in bad user experience and customer calls
- Network security services on Home routers may not have the capability to detect new emerging and sophisticated attacks.
    - Infected device can also be used for crypto-jacking and compromises home user security and privacy.

Solution Overview: Call Home



DOTS server
(CPE)

DOTS client
(ISP)

(D)TLS connection initiated by DOTS server (Idle time)

Attack traffic from compromised device(s)

Mitigation request conveying the attack traffic information

Identify the infected device, inform the user, isolate the device and block traffic to attack target

Mitigation response

Updates from 01 to 03

- DOTS server maintains a single DOTS signal channel session for each DOTS-capable upstream provisioning domain
  - Single DOTS session established during idle time
- If CGN is located b/w the DOTS client and server domains, only internal IP addresses/prefixes must be communicated in the mitigation request
  - External IP address is not visible to the DOTS server
  - RFC8512 and RFC 8513 define YANG modules to retrieve the internal IP address and port number mapped to external IP address and port
  - If MAP or lwAFTR is enabled, source port numbers are used to identify the home network generating the attack traffic

Updates from 01 to 03

- If translator is enabled on the DOTS server, find the internal source IP address and MAC of the compromised device
    - ➢Inform the user, isolate the device and block traffic to attack target

Updates to Security Considerations

- DOTS servers may not blindly trust the mitigation request from DOTS clients, e.g.,
  - Enable DPI to inspect all the traffic from the compromised device(s) to the target
  - Re-direct/clone the traffic from the compromised device(s) to the target to a DDoS Detector or DDoS mitigation system
  - Seek consent of the DOTS server domain administrator to take appropriate mitigation action

Updates to Privacy Considerations

- The Call Home extension does not leak any new information that can be used to ease surveillance:
  - ➢DOTS Call Home extension is only advisory in nature
  - ➢DOTS servers do not share the compromised device details with the DOTS client(s)
  - ➢Cross-validation of the attack by the DOTS client
  - ➢Administrator consent
  - ➢Protect both the target resources and home networks with compromised devices launching the DDoS attack

Next Step

- All comments were addressed
- Stable version
- Request WG adoption of the draft

- Comments, Question and suggestions?