DDoS Open Threat Signaling (DOTS) Working Group

Operational Requirements

Chris Morrow <morrowc@ops-netman.net>
Network Security Engineer, Google

Roland Dobbins <rdobbins@arbor.net>
Principal Engineer, Arbor Networks
Introduction & Context
What is a Distributed Denial of Service (DDoS) attack?

- An attempt to consume finite resources, exploit weaknesses in software design or implementation, or exploit lack of infrastructure capacity
- Targets the availability and utility of computing and network resources
- Attacks are almost always distributed for even more significant effect (i.e., DDoS)
- The collateral damage caused by an attack can be as bad, if not worse, than the attack itself
- DDoS attacks affect availability! No availability, no applications/services/data/Internet! No revenue!
- DDoS attacks are attacks against capacity and/or state!
Three Security Characteristics

- The goal of security is to maintain these three characteristics
Three Security Characteristics

- The primary goal of DDoS defense is maintaining availability in the face of attack.
Realities of Coordinated DDoS Defense
Common Perception of Internet Security Posture Today
Actual State of Internet Defenses Today
Who Can Help?

Your ISP or MSSP!
How Can You Ask for Help Today?

Technology pioneered by Robert Hooke in 1667, only slightly improved!
Asking for Help is Hard! Knowing How to Help is Harder!

• Most end-customers have no idea what their normal Internet traffic looks like, much less what’s actually happening when they’re being DDoSed (or even understanding that they’re under attack!).

• Many ISPs/MSSPs do not provision DDoS defenses in detail for their end-customers. In many (most?) cases, end-customers cannot articulate what servers/services need protection, what network access policies should be in place, etc.

• This drastically slows reaction/mitigation times.

• This drastically impedes reaction/mitigation efficacy.

• This leads to extended outages, lost revenue, frustrated end-customers (and customers of those end-customers).
Automated DDoS Attack Notification Methods Exist Today

- But they are proprietary!
- End-customers can’t mix-and-match vendors, ISP DDoS cloud mitigation providers, MSSP DDoS cloud mitigation providers. Effective coordination during an attack is for all practical purposes impossible.
- Servers/services/infrastructure devices which are the targets of DDoS can’t signal for mitigation, even if they have the ability to detect and classify DDoS attacks (think Apache mod_security/mod_evasive, BIND RRL).
- ISPs/MSSPs must coordinate (badly, inefficiently) manually when jointly working to mitigate DDoS attacks.
- As attackers shift DDoS vectors/resources, severe latency, common miscuing occurs between defenders.
- Web portals exist; they’re specific to vendors/ISPs/MSSPs, have varying degrees of mitigation configurability (most end-customers wouldn’t know what to configure), and can be difficult to access during an attack when IDC & client LAN transit are conflated.
DDoS Defense Becomes a Typing Contest . . .

Attacker.
DDoS Defense Becomes a Typing Contest . . .

Defender.
Largely Static, Low-Agility Defenses . . .
... Lead to Predictable Outcomes.
Coordination of DDoS Defenses, Circa 1995.
Coordination of DDoS Defenses, Circa 2005.
Coordination of DDoS Defenses, Circa 2015.
We Can – and *Must* – Do Better Than This!
We Need a Standardized Way of Sharing Information . . .
. . . Across a **Reliable** Transport That Will Make It Through **Policies** . . .
. . . That Can Be Relayed Internally and Externally as Needed . . .
... Everyone and Everything on the Network Can Participate ...
... In Coordinated, On-Demand DDoS Defense.
Summary of DOTS Operational Requirements
DOTS Operational Requirements

• Standards-based exchange of DDoS attack and mitigation information.
• Must not assume organic detection/classification capabilities of supplicant.
• Must work across common unreliable and reliable transports.
• Must support mutual authentication and optional crypto.
DOTS Operational Requirements (cont.)

- Must **describe target under attack** (IP address range, ports/protocols/services running on target, etc.).
- Must **describe desired outcome** in general terms (block, redirect, scrub, rate-limit, etc.).
- Must **update supplicant** with implemented actions and status, supplicant must do same.
- Must support **intra- and inter-organizational relays**.
DOTS Operational Requirements (cont.)

- Must support policy-based action/outcome filtering and transformation.
- Must be extensible.
- Must focus on DDoS initially, other uses can come later.
- Must minimize complexity of implementation and node interaction.
DOTS Operational Requirements (cont.)

- Must include a ‘heartbeat’ function.
- Must be detection/classification/mitigation-technology agnostic.
- Must support allowed distribution scope (TLP?).
- Should utilize existing protocols and information models wherever possible and whenever appropriate.
This Presentation – http://bit.ly/1I2IVrF
DDoS Open Threat Signaling (DOTS) Working Group

Thank You!

Chris Morrow <morrowc@ops-netman.net>
Network Security Engineer, Google

Roland Dobbins <rdobbins@arbor.net>
Principal Engineer, Arbor Networks