Virtual Absorption of DDOS Attacks

Dr. Edward G. Amoroso
Chief Executive Officer, TAG Cyber LLC
Mob: (201) 454 – 1854
eamoroso@tag-cyber.com

Abstract

Traditional DDOS attack protection involves the scrubbing of packets at Layer 3, with advanced detection and blocking of attacks at Layer 7. With the adoption of virtualization and cloud services in the enterprise, newer virtual security techniques are now required for absorbing DDOS attacks. *(Analyst Note: This paper was inspired by separate discussions with Sam Curry of Arbor Networks and Tushar Kothari of Attivo Networks in 2016.)*

Introduction

The evolution of distributed denial of service (DDOS) attacks has progressed considerably from its primitive beginnings in the 1990's. At the time, denial of service involved little more than simple TCP/IP shenanigans such as SYN floods aimed at an IP address. Recently, however, these attacks have moved into much more dangerous territory with botnet-originated, enormously high volume streams of packets designed to take out a Website. Such attacks often include clever domain name service (DNS) manipulations of the botnet command and control, which makes takedown a difficult task.

In 2012, these attacks became big news across the finance industry as a group purported to originate in the Middle East used a relatively simple botnet called Brobot to wreak havoc for several weeks on the public-facing sites of several banks. Service providers, security solutions providers, and the banks themselves, all scrambled to deal with these attacks, with varying levels of success. Eventually, things subsided as a result of combined improvements in security with the decision on the part of the attacker to stand down.

The whole experience left a bad taste in the mouths of everyone involved, and as one would expect, also saw an expansion in investment for companies working to stop DDOS attacks. In 2012, Arbor Networks and perhaps one or two other small companies offered platform solutions to thwart DDOS attacks, mostly at layer 3 in the OSI stack. Today, the number of vendors has grown several fold, usually with the value proposition of solid layer 3 protections with extensions to layer 7 attacks targeting application compute logic. In spite of the emergence of these newer vendors, virtually every cyber security expert today would refer to the DDOS threat as *unsettled* – at best.

Modern DDOS Protections

The security solutions used to stop previous DDOS attacks involve some sort of man-in-the-middle monitoring and processing designed to use simple Turing tests to identify automation, and to then divert all traffic to a place where it can be effectively scrubbed. The goal is for the good traffic to be passed along to the desired destination, with the errant traffic stopped by the scrubber. Since this involves a fair bit of heavy lifting at the routing layer, we call the attack and the corresponding security Layer 3 DDOS, in reference to the positioning of routing on the OSI stack.

Figure 1. Modern Layer 3 DDOS Protections

The emergence of Layer 7 attacks directed at Web applications was a natural offensive progression as the bad guys realized what was going on with scrubbing. By employing clever tricks that understand exactly how an application works, the adversary suddenly ha a new arsenal of disruptive weapons. While there are unlimited use-cases for Layer 7 – which, incidentally, is one of the reasons application level attacks are harder to stop than Layer 3 floods – a common case involves egress amplification.

The way this attack works is that the intruder locates some exploitable aspect of the target application where an Internet-accessible query/question/probe results in a high-volume response. By hitting the soft spot repeatedly, the response builds into a mini-denial of service condition that fills the egress link from the application back out to the perimeter gateway.

Figure 2. Example Layer 7 Egress Amplification

The