Chapter 8

Protecting the E-Commerce Website against DDoS Attacks

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

A DDoS attack attempts to reduce the ability of a site to service clients, be they physical users or logical entities such as other computer systems. This can be achieved by either overloading the ability of the target network or server to handle incoming traffic or by sending network packets that cause target systems and networks to behave unpredictably. E-commerce sites are popular targets for attack for a number of reasons. The complexity of the site can reduce security coverage through human error, design fault, or immature technology implementations. E-commerce sites have a large presence and are easy to access. Defending a site against DDoS requires security teams to adopt a consistent and focused approach. In particular, staying aware of current security issues and new attack methods is of particular importance. Ensuring a reasonable security profile is an ongoing and dynamic process requiring continual refinement and consideration.

INTRODUCTION

Many knowledge experts have described the current era as the information age—the dawn of a bright new future, a time when the barriers to communication have been dismantled, allowing the formation of virtual communities that span the globe. Businesses now have the ability to project their presence beyond the normal confines of geography, enabling them to reach out to a market that years earlier they would have, by necessity, ignored. Recreational users of the Internet share information and experiences almost instantly with people a world away. The application of Internet technology and the associated opportunities seem endless. And that is part of the problem. With every opportunity comes risk. In the world of the Internet, this risk often materializes in the form of security. The Internet and security are inextricably linked—one should always accompany the other. Security should always be a byword when using the Internet, but some believe the mere use or integration with the Internet eliminates the ability to be secure in the first place.
Security is an evolving field where the good guys always seem to be one step behind the bad. The list of security risks a security officer or administrator may have to contend with reads like a science fiction novel. In a single week, they could be expected to counter threats posed by highly contagious viruses, Trojans, worms and even be attacked by Zombies. Recently one of the newer additions to the security officers’ lexicon of despicable terms was the highly publicized Distributed Denial of Service (DDoS). The end of 1999 brought to light a scenario that security experts around the globe had predicted but had hoped would not arise. New tools for performing Denial of Service (DoS) attacks on a massive scale were released to the Internet. These new tools were referred to as DDoS tools because of their distributed nature. They allowed an attacker to coordinate attacks against Internet sites from client machines (often called zombies) distributed around the world using a single client program. Given enough zombie machines, an attacker could bring any site to its knees.

As the security community scrambled to alert the world to the dangers these tools created, the assaults began. In just a few short days, the foundations of some of the largest Internet sites were rocked by massive coordinated attacks. The conditions that had set the stage for the spate of attacks had been in place for quite some time. Bandwidth had become a commodity, with broadband access offering high-speed Internet connectivity through cable modems and digital subscriber lines (DSL). Most computing communities were blissfully unaware of the dangers they faced. Penetrations began occurring at an alarming rate, leaving behind massive networks of DDoS zombies for later use. In addition, many of the largest sites on the Internet had failed to implement some of the most basic protection mechanisms. This confluence of technological advancement and circumstance allowed a single David to knock down several Goliaths with one powerful stone—DDoS.

**WHAT IS A DDoS ATTACK?**

To understand a DDoS attack and its consequences, we first need to grasp the fundamentals of DoS attacks (Ghosh, 2001; Russell, 2001). The progression from understanding DoS to DDoS is quite elementary, though the distinction between the two is important. Given its name, it should not come as a surprise that a DoS attack is aimed squarely at ensuring that the service a computing infrastructure usually delivers is negatively affected in some way. This type of attack does not involve breaking into the target system. Usually a successful DoS attack reduces the quality of the service delivered by some measurable degree, often to the point where the target infrastructure of the DoS attack cannot deliver a service at all. A common perception is that the target of a DoS attack is a server, though this is not always the case. The fundamental objective of a DoS attack is to degrade service, whether it be hosted by a single server or delivered by an entire network infrastructure.

**Laying the Groundwork: DoS**

Before the DDoS hue and cry rose to almost thunderous proportions, DoS attacks had been tirelessly aimed at networks for some time. DoS attacks are conducted using software written to deliberately cause degradation in the target systems service levels. A number of well-documented types and variants of DoS attacks currently swirl around the backwaters of the Internet. One of the significant problems exacerbating DoS attacks is the number of freely available programs that turn this technical exploit into a task that