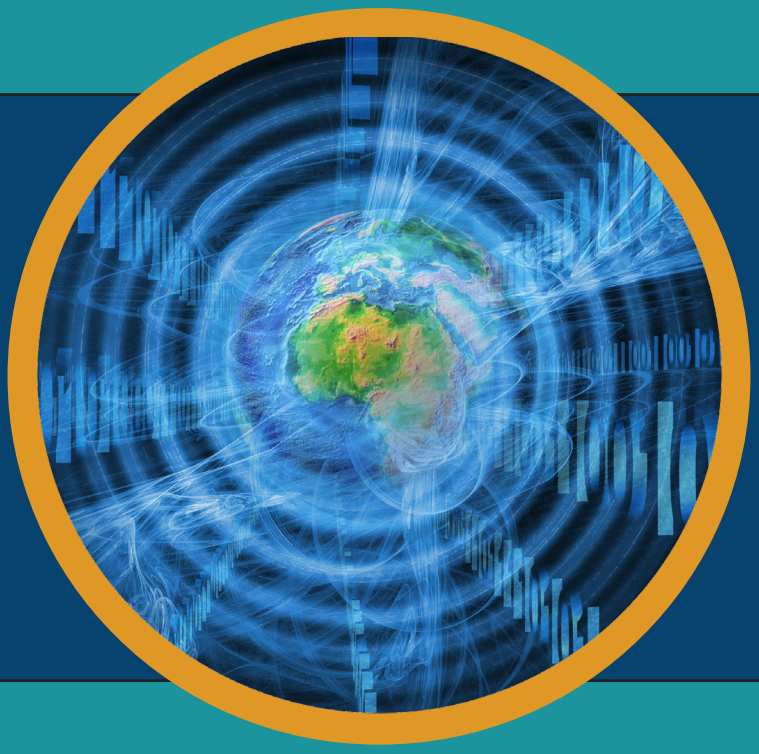
Understanding DDoS Attacks & Mitigation Strategies

Four Critical Elements for an Impermeable DDoS Defense



Introduction

DDoS attacks have been a nuisance for websites, companies and Internet Providers for years. In these attacks hackers have employed several methods over time to effectively shut down websites for a variety of reasons. In this paper, we'll explore how these attacks happen, who commits them and why, and what can be done to counter them.

What is it?

DDoS stands for Distributed Denial of Service. In layman's terms, it refers to overwhelming a network or website with counterfeit traffic and causing it to be unreachable by the user. Of course, any website can get overwhelmed without a DDoS attack simply by getting more visitors than it can handle, where bandwidth to a server is not sufficient or the server is unable to accept any more connection requests. This may happen during certain times, such as Amazon Prime Day, or a popular live streamed event. Hackers quickly found out that they can use this vulnerability as a way to purposely shut down websites or networks. These attacks can come in different ways, and each one can be devastating to an unprepared target.

Common Types

The most common type of DDoS attack is a "volumetric" attack. These attacks start with creating a "botnet" or gaining access to an existing one. A botnet is a group of remote computers that have been compromised by spyware or malware. The hacker can direct this group of zombie computers to simultaneously contact the target system, eating up the available bandwidth and causing actual visitors to be unable to reach the site.

To increase the impact of the attack, the zombie computers can also make use of "reflectors" to amplify the attack. In this case, rather than attacking the target directly, the zombie computer sends a standard request to a vulnerable server that uses the UDP protocol, like a DNS or NTP server. But, instead of using its own IP address as the source address in data packet, the zombie computer spoofs the IP address of the target computer as the source address. When the UDP server gets the request, it unwittingly sends the reply to the target computer. This can greatly amplify an attack, because a small UDP request sent to a server can

generate twenty times or more the amount of data back to the source IP address. For example, a simple request for a "start of authority" (SOA) record from a DNS server will send a much larger reply to the source address. In an amplified attack like this it doesn't take a large botnet to leverage a few compromised DNS servers to overload the bandwidth of the target network and make it unavailable for others.

Another way that DDoS attacks are launched is by exploiting weaknesses in the protocol layers in the network stack, leaving a server or application unavailable for access. These types of attacks have different names for different angles of attack. A "SYN Flood" targets the TCP connection, creating an overload of partial connections before they can time out, thus clogging the network bandwidth. Attacks also take place at the application layer (Layer 7). For example, if a hacker uses their botnet to send multiple requests to log in to a website, it can overload the servers and make login requests from actual users time out.

What's in it for the Hackers?

The motives behind DDoS attacks have evolved over time. There are the obvious reasons you might expect someone to launch an attack, such as a former, disgruntled employee of the target company taking some measure of revenge. For others it might be to make a political statement or simply to cause chaos and anarchy online. Recently, many DDoS attacks have been used for the purpose of extortion or theft. With the onslaught of debilitating attacks that have happened, a simple threat and a packet of data can be all that's needed to get a company to pay money to protect their network. In addition to direct extortion, a DDoS attack can also be used as a diversionary tactic to draw the attention of a company's IT staff away from a hacking attempt. While everyone is distracted by working to block the DDoS attack, the hacker has a better chance of getting into the network unnoticed to steal data.

Solutions

As security experts have considered how to counter these attacks, several solutions have been developed over time to respond to the vulnerabilities in these systems. Three typical deployment methods are Proactive, Reactive, and Hybrid models.

A Proactive deployment involves the systems being configured to check 100% of the inbound traffic and being ready to mitigate anything it sees as out of the ordinary or malicious. By putting detection appliances in-line at the edges of their network, businesses are able keep watch over the full spectrum of the network traffic. This provides high accuracy and fast response, but can be an expensive solution in large networks.

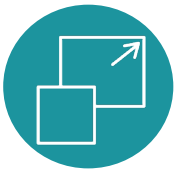
A Reactive deployment uses the NetFlow data that is already available from the network edge routers and switches to get some level of traffic visibility. In this method, the mitigation device is placed in the traffic path only when you detect a DDoS attack. While this is a more cost-effective solution, the traffic visibility available via NetFlow is less granular, so it can also miss some events, and the response for mitigation of the DDoS event will be slower.

There is a "hybrid" model that uses the strengths of the proactive and reactive methods to detect and mitigate threats. In this type of solution a less expensive in-line device is placed in the network to detect and mitigate smaller network or application layer attacks. If a volumetric attack is detected that would exceed the network's capacity, all traffic is diverted to a cloud-based service that then scrubs the traffic before returning it to the targeted network.

With the rise in DDoS attacks, companies will need to be prepared and may need to re-evaluate their current defenses. There are four factors that can be considered when making a decision on what type of DDoS system to deploy – ***Precision, Scalability, Efficiency and Affordability.***

Precision

Precision is necessary to avoid false positives and negatives, potentially missing threats, or hindering legitimate traffic. The primary reason to deploy DDoS protection is to maintain service for legitimate users during a DDoS attack by stopping the attack and not adversely affecting normal traffic. If legitimate users cannot access the network, then the solution has failed. An effective DDoS defense must be able to intelligently distinguish between legitimate users and traffic from attacking botnets.



Scale

When it comes to scale, the advance of technology has brought a new element into the picture – the Internet of Things. These ubiquitous devices are typically always running and connected to the Internet, meaning that they are always potentially vulnerable. Whereas once only computers were the possible devices to be used in a botnet, now there is a whole slew of network-connected IoT devices that are ripe for exploitation. A DDoS solution must be able to react to the intensity of the attack as far as volume of packets per second, as well as the breadth that is now possible with the millions of geographically distributed IoT devices that could potentially be compromised and used to attack a network.

Efficiency

In terms of efficiency and manual intervention, automation in a DDoS system is a significant benefit. Older DDoS solutions require a lot of manual intervention, which pulls staff off their normal jobs to fight fires. Plus, quite often when there is one attack, multiple attacks will follow. A solution should be chosen that has an automated escalation process, so potential threats can be detected and mitigated programmatically. This will eliminate much of the manual intervention and drain on network staff that otherwise would be required to defend against attacks.

Affordability

Of course, affordability is important. Companies can only do so much with the internal resources they have within a limited IT budget. Fighting off DDoS attacks can become an expensive endeavor depending on how it is handled. A solution that is high-performance but compact will reduce the total number of appliances needed to meet your organization's capacity requirements. This not only reduces hardware costs, but also power, cooling and space requirements in the data center. If you use a cloud-based solution, a vendor that does not charge for the amount of traffic in an attack or how many IP blocks are used would be a good choice.

The Bottom Line

With the number and severity of DDoS attacks continuing to grow, companies need to be prepared to defend their network and their assets against the threat of a shutdown and theft. While network security like DDoS mitigation is a budgetary item that doesn't provide a direct return to the bottom line, the cost of failing to protect your network from an attack can be much higher in the long run.

Additional Resources

For more information, visit our website and check out two of our Product Sheets:

A10 DDoS Attack Solution-Protection and Mitigation

Corero SmartWall DDoS Protection

ZCorum™

ZCorum provides broadband Internet and communication solutions to telcos, cable companies, utilities, and municipalities, assisting in all facets of broadband implementation, integration, engineering and consulting, network monitoring and diagnostics. ZCorum also offers wholesale, private-labeled Internet services, including data and VoIP provisioning, email, Web hosting, and 24x7 support for end-users, enabling service providers to compete effectively in their local rural and suburban markets. ZCorum is headquartered in Alpharetta, GA. For more information, please visit ZCorum.com or contact us at 1-800-909-9441.

4501 North Point Parkway, Suite 125 | Alpharetta, GA 30022 | Phone: 800.909.9441 | info@ZCorum.com