Information Security Services

Preparing for Distributed Denial of Service (DDoS) attacks
An Introduction to DDoS attacks

After emerging in 1999, Distributed Denial of Service (DDoS) attacks have again gained a lot of attention due to recent high-profile attacks by hacktivist groups and extensive media coverage. As a trusted security services provider, Dell SecureWorks has prepared the following high-level brief to provide a basic understanding of these types of attacks, and methods that can be used to mitigate them. Those interested in a more detailed technical analysis should look to the end of this paper for a link to the complete Dell SecureWorks Threat Analysis of DDoS.

DDoS attacks are attempts by one or more adversaries to disrupt availability of a network asset using multiple attack sources. This can occur at the network layer when available bandwidth is consumed, at the transport layer when processing capacity of in-line network devices is exceeded, or at the application layer when the ability of an application to respond to network requests is exceeded.

Recent high-profile attacks have targeted Web servers at the application layer, where one or more adversaries attempt to take down a website by flooding the Web server with more traffic than it can handle. A successful DDoS attack against a Web server can effectively knock the website offline, making it unavailable to end users and customers. These attacks are most often used to damage businesses whose websites or online assets are a major source of revenue, an indicator of brand value, or critical to business operations. An organization can become a target for any variety of reasons, but the attacks are often used as a form of protest by activists or an attempt to extort a business by essentially holding its website hostage.

Although major DDoS attacks are a rare occurrence for most organizations, they can be very detrimental and attempts cannot be prevented. Because of this, it is important to proactively implement mitigations and practice DDoS incident response plans prior to a DDoS event occurring. The remainder of this brief will outline the steps that a business can take to mitigate the effects of a DDoS attack.

Basic DDoS Preparation

DDoS attacks are possible because the Internet is built from limited consumable resources. If a business had unlimited bandwidth and unlimited computing resources, then an attacker couldn’t feasibly consume all of these resources - but this simply isn’t the case. An organization must balance the amount of resources they are willing to put towards preventing a DDoS attack from occurring with an acceptable level of risk.

Security professionals, especially those well versed in DDoS, can usually help the organization compute the costs associated with the different levels of risk. The more resources (i.e. Web server capacity and Internet bandwidth) an organization has dedicated to their public-facing website, the more difficult it will be for an attacker to consume all available resources. Therefore, the business must determine and understand the level of risk associated with their infrastructure and how easy or difficult it would be for an attack to be successful.

Organizations must consider the varying components of the network architecture during this review, because there are often multiple points of failure that could collapse under the pressure of a DDoS attack. These technologies often come with numerous configuration options and bypass controls that can be set up to align with the security needs and risk tolerance of your organization. As a starting point, determine the weakest link and first point of failure in your network by performing load testing.
and a system performance review. This analysis highlights areas where investment can be most effective at preventing the downtime that would result from a DDoS attack. It is also critical that a business review and understand the full cost of website downtime, so it can be taken into consideration when calculating how much to spend on the resources to prevent these attacks.

Understanding and agreeing upon these metrics is not a simple task, nor is designing and implementing the right architecture and policies. If your internal resources do not have the necessary time or expertise to perform these tasks, the Dell SecureWorks Security and Risk Consulting (SRC) group can help by evaluating your current environment and providing recommendations that will best meet your needs and budget.

**Creating an Incident Response Plan**

Internet resources are limited, so complete DDoS prevention is impossible in practice. Therefore, a determined attacker may be able to successfully take down a website built on a very resilient architecture. Nowadays, there are publicly available toolkits that make attacking a target quite simple, so that attacks are not limited to groups with a sophisticated knowledge of networking and architecture design. Thousands of botnets are available for rent on the Internet, providing ample resources for those who would want to disable a public-facing website.

It is for all these reasons that DDoS attack mitigations should be part of the organization’s incident response, crisis response and business continuity plans. Having a plan of action in place is critical to ensure a timely recovery from a successful DDoS attack. This plan of action should be practiced and tested regularly to ensure that everything goes as expected and alterations can be made to improve processes and efficiency.

Because successful attacks can have an impact on multiple business units, all stakeholders need to be made aware of the consequences of DDoS attacks and included in the planning process to ensure their interests are properly represented and protected. Typically, an organization’s CIO, CSO, CISO, or Risk Management Officer will ultimately be responsible for ensuring this representation happens, and in the event of an attack that significantly impacts multiple business areas, will likely be the one held accountable for the outcome.

The Dell SecureWorks Security and Risk Consulting team can help organizations build an incident response plan that maps to their environment and staffing model. Their expertise and experience in responding to DDoS attacks can provide insight into best practices and common pitfalls. During a typical DDoS Incident Response Plan engagement, the SRC group can help you:

- Understand what your Internet Service Provider is able to do at the provider level
- Understand the limitations of the networking and information systems in your architecture
  - Identify the ‘weakest link’ in the network
  - Ensure proper device configurations for identification and mitigation of attacks
  - Analyze the cost and benefits of increasing website capacity and resources
- Outline escalation and notification procedures when a DDoS attack is identified
- Record roles and responsibilities during an attack
- Document techniques for identifying the type and source of a DDoS attack
• Record detailed mitigations for various types of attacks - such as implementing strict SYN limits per IP, geographic blocking, or reducing the per-client connection limits at the ASA bundle
• Plan for the public response and communications that will need to occur
• Create an outline for a follow up and lessons learned report
• Additional agreed-upon tasks as requested by the customer

Conclusion
DDoS attacks cannot be prevented, but organizations can become aware of the threat and work proactively to establish countermeasures and incident response plans to mitigate and minimize the potential impact of a determined and well-resourced attacker. Understanding the adversary’s tactics, techniques, and procedures, as well as the options available for mitigating the effects, is vital to establishing a strong security posture and planning a rapid, effective response.

A more detailed technical analysis of DDoS attacks is also available, describing the various types of attacks, common tools and tactics, trends in DDoS, countermeasures, and legal issues. The analysis is targeted towards an audience with a solid understanding of networking. The report is available at:

Threat Analysis: Understanding and Combating DDoS Attacks

Should you have any additional questions about how Dell SecureWorks can help your organization plan for or respond to DDoS attacks, contact your account manager, email info@secureworks.com or call (877) 905-6661.