Understanding & Preventing

DDoS Attacks

(Distributed Denial of Service)

A Report For Small Business

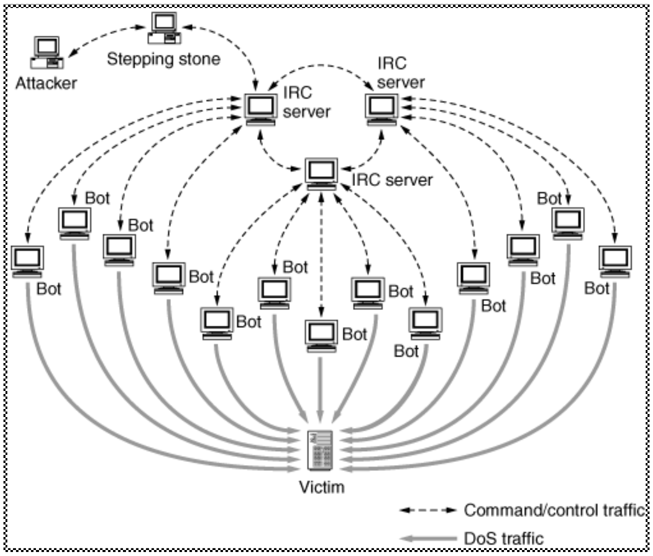
According to a study by Verizon and the FBI published in 2011, 60% of data breaches are inflicted upon small organizations!

The HelpDesk LLC

Topics Covered In This Report

What Is A DDoS Attack?

Let's start with Denial Of Service or DoS. A DoS attack is a malicious attempt by someone to make a website unavailable to its intended users. The typical attack usually involves sending an extraordinarily large number of requests for information to the web host. In a typical legitimate connection, the user sends a request for authentication to the server. The server then returns the authentication approval to the user. The user acknowledges the approval. Then, the server allows the user to access the web server. In a denial of service attack, the user sends several authentication requests to the server, filling it up. However, all of the requests have false return addresses. When the server can't find the user, it tries to send the authentication approval again. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again–tying up the service indefinitely. The goal is to tie up all of the server processing time.



Another layer of complexity in defending against these attacks is a Distributed Denial of Service Attack, or DDoS. In a DDoS attack, the attacker first creates and "army" of zombie individual computers that act as robots and upon command from the attacker, simultaneously launch a coordinated attack on a given website. In a DDoS attack, it is more difficult to identify the originating attacker, since they are hiding behind the army of zombie PC's. The attacking PC's are typically referred to as a botnet. In other words, they represent a network of robot PC's. The botnet army can number in the tens, hundreds or even thousands! The larger it is, the more damaging the attack can be on the victim. The main goal is to shut the server down with many simultaneous requests.

Botnets are created through the distribution of malware, spyware, and deceptive requests for information from unsuspecting legitimate users. The users usually inadvertently download a malicious piece of code to their computer, thinking that they are responding to offers from legitimate companies. The reality is, they are downloading malicious code. The malicious code then converts their PC into a slave or robot, ready to receive instructions from a remote master. When the master sends a signal, the slave PC begins to launch attacks on the targeted victim website. This DDoS style of attack keeps the attacker well hidden from the victim website, making it difficult for the victim to identify the source.

Unfortunately many web hosting companies, particularly small companies are not prepared to defend against this style of attack. When the attack comes, all the hosting company knows is that there is "a lot of traffic to the site." As it increases, their typical solution is to increase bandwidth. Increasing bandwidth allows increased attacks, the problem persists and eventually the site comes down. The typical small hosting company is mainly concerned with protecting their own equipment and clients. If they cannot or do not know how to protect against DDoS attacks, their solution oftentimes is to tell the client that they will have to find another host.

Although there are many types and strategies for DDoS attacks, which will be discussed later in this report, there is usually a single simple main goal--that is, to flood the website service with so many requests that it either slows or crashes the site. Generally, the goal is not to steal data. Rather it is to undermine the ability of the provider of the website to deliver services to their end users.

How to Tell When Your Website Is Under Attack

The typical symptoms that indicate your website is under attack are easy to recognize. An unusually high number of requests are usually the first sign. The number of requests will continue to increase. The website response time gradually drops. Eventually users get no response from the site at all. There may also be an unusual number of spam e-mails received. There may be traffic problems with related routers around the victim server. Excessive usage of resources by the server hosting the website is not uncommon. Disruption of configuration information on peripheral equipment, routers, unsolicited resetting of TCP sessions, and excessive consumption of bandwidth are all common signs and symptoms of a DoS or DDoS attack.

Why Organizations Come Under DDoS Attacks

There are many reasons that organizations come under attack. Most generally fall into one of a few categories: political, religious, or competitive. It's not always easy to understand what drives the bad guys. Sometimes crime is random. But many times it is driven by a motivation that most of us understand. Here is a short list of reasons to help you think about how susceptible your website may be to an attack:

- **Blackmail--**the attacker wants to hold your website hostage until you pay a large sum of money or provide some other payoff.
- **Principle Driven--**the attacker does not agree with your morals, principles or values and thus wants to hinder or eliminate your effort to promote them.
- **Competition--**the attacker is one of your competitors or has been hired by one of your competitors to thwart your business operations.
- **Politics--**There is no shortage of opinions in the world on how governments, communities and cultures should operate. Wars have been fought because of these differences.
- **Hate Crime--**Entire books have been written about the rise of this category over time.

- **Electronic Protests--**Oftentimes this is related to the rejection of a user or groups of users. Here, the attacker is attempting to retaliate for some change in your business model or other unagreeable action.
- **Experimenting--**Attackers may simply come after your website just to see if it can be done.
- **For the Challenge--**This is similar to experimenting, but here they may be trying to prove a point to themselves or someone else.
- **Software Bug--**This is more rare, but there may be a bug that is causing too many users to come to your website.

Understanding The Different Types of DDoS Attacks

Many attacks use a SYN Flooding method. SYN stands for synchronization. A SYN packet is sent from a hostile attacking computer (or botnet zombie computer) to a server using fake IP addresses. When the attack begins the server sees multiple attempts by the attacker to establish communications. With each attempt the server responds with an acknowledgement in an attempt to get a "handshake." But, because the IP addresses are fake, the handshake never occurs. The server port remains open and waiting for a short period of time. Before it closes, another SYN request is sent by the attacker. The cycle continues until the server's processors are bogged down with requests. Keep in mind that there are lots of variations of this type of attack. As defenses are developed the bad guys continue to dream up new alternative methods of attack. The following table outlines a few of the most common that have been used in the past.

Flood Type	Description	Degree of Difficulty for Attacker	Degree of Difficulty Of Stopping	Mitigation Notes
SYN	False packets fill connection to server	Low	Medium	Low volume floods are easily stopped by firewalls.
Zombie	Same as above, however number of packets increase exponentially.	Medium	High	Requires specialized logic and equipment for behavioral mitigation and rate limiting.
ICMP	A specific type of packet used to overload the server and the pipe.	Low	Medium	Low volumes can be stopped by routers. Higher volumes require special equipment.
Non-Service Port	TCP/UDP packets overload server and pipe on ports not in use.	Low	Medium	Low volume can be stopped by routers. High volume requires special equipment.
Service Port	Packets overload server and pipe on ports that are in use.	Medium	High	Firewalls, switches and routers cannot stop. Special equipment required.

Flood Type	Description	Degree of Difficulty for Attacker	Degree of Difficulty Of Stopping	Mitigation Notes
Fragment	Fragmented packets sent to overload the server.	Low	Medium	Firewalls, switches and routers cannot stop. Special equipment required.
HTTP Get	Bots overload server and pipe on service ports mimicking legitimate users.	Low	High	Firewalls, switches and routers cannot stop. Special equipment required.
Blended	Combinations of all of the above are used simultaneously.	High	High	Firewalls, switches and routers cannot stop. Special equipment required.
Anomalous	Abnormal or packets with unusual headers are sent to overload server.	Low	Low	Some firewalls can stop these attacks. Special equipment routinely stop this type of traffic.
Regional	Bots in an identified pattern or region attack.	High	High	Special equipment will identify pattern and stop the attack.

The above table is not comprehensive. There are many other variations of attacks. The level of sophistication of the attacks continues to escalate. As each year goes by the need for more specialized equipment to avert the attacks continues to increase.

Why You Should Protect Yourself

If you are reading this, you are likely involved with a business or an organization that uses and relies on the Internet and your website to service your members, customers or constituents. Most businesses will suffer within a short period of time if their website is unavailable or inaccessible. The following highlights a few of the reasons that every business and organization with website users should seriously consider a DDoS protected web hosting arrangement with their service provider.

- **Your Reputation Is At Stake!** Within minutes a botnet attack can ruin your reputation with customers, clients or constituents. They expect you to have adequate protections in place!

- **The Cost Of Lost Business!** Lengthy attacks cannot only cost you in downtime but also lost business. You can't afford to be without the latest in protection technology!

- **The Cost of Recovery!** The cost of recovery from an attack will be more than the cost to protect from an attack. This means if you decide to "self-insure" you will regret it later.

- **Most Web Host Providers Are NOT Security Experts!** The complexity of broadband web attacks escalates daily. Most host providers are not equipped to handle attacks! The bad news is that when your site comes under attack the typical web hosting provider not only does not know how to identify the attack, they also don't know how to stop it once it begins.

  First, they will tell you that <u>your</u> website is causing a traffic problem on <u>their</u> server. Next, when things get worse, they will pull your website offline to protect their server and their other customers. The reason is that most small hosting companies are using shared environments, where traffic increases with one website will slow response time to other websites in the same environment. If your business critically relies on access to your website, you don't want to risk not being protected.

- **Your Website Is A Valuable Asset!** This is especially true if you have an e-commerce business model. Today, most websites are at the heart of the business. They need to be protected!

- **You Could Lose Customers!** When your website goes down you lose credibility. Your business may be viewed as unreliable and unprofessional. Depending on other options that your customers have, they may choose to leave and do business with your competitors.

- **DDoS Protection Is Not For The Inexperienced Or Faint Of Heart!** The level of attack sophistication has increased dramatically in the past few years. Proper protection requires a major investment in equipment, software and specialized skills that the average web host simply doesn't make to protect their clients. If your company or organization is vulnerable to attacks, a question about the level of protection that the host can provide should be the first thing to ask. Be sure that your host has proper equipment for an adequate level of protection for your website.

What Are The Options For Protecting Your Website?

There are three general strategies that most companies use to protect their websites from Distributed Denial Of Service attacks. They are: 1) increasing bandwidth, 2) attempting to "beef up" with traditional infrastructure solutions and 3) using a host with professional mitigation services. Each of these three solutions will be addressed here separately.

Increasing Bandwith--Overprovisioning on bandwidth can be expensive and is not always the most reliable solution. As everyone knows bandwidth costs money. So, the more you need the more you pay for. The general idea here is that you purchase enough bandwidth to accommodate your normal traffic and then you buy more to accommodate any malicious traffic from an attack. In theory this seems like a good strategy. However the number of botnets and slaves within those botnets is growing every day. That means the size of the attacks is on the increase. So the amount of bandwidth you must purchase keeps increasing. And further, the amount that you think you need may still not be enough depending on the size of the attack. A sizable attack may still easily overwhelm your computing resources.

Using Traditional Infrastructure--Firewalls and routers with rate limiting and access controls are the traditional solution. Limiting concurrent sessions does lower the bandwidth to the server. And, these methods may work effectively on small attacks. But limiting concurrent sessions still may allow the sessions that are created to do considerable damage. This is especially true in the face of increasingly larger botnets numbering in the thousands. That means a strategy of increasing bandwidth must be combined with an increase in hardware in the infrastructure. This is usually an infrastructure investment that companies do not want to make. And even when they make the investment it is not enough for the modern day botnet.

Professional DDoS Protection Hosting--In today's environment this is the only solution that makes sense for small business. The typical small local hosting company will not have the infrastructure, bandwidth or special equipment to protect their servers. This makes small business and small organizations especially vulnerable to DDoS attacks. Using a qualified host will be less costly than buying more infrastructure hardware and overprovisioning on bandwidth. A hosting company with DDoS protection in place will have the specialized equipment in place to scrub and clean the traffic to its servers, thus eliminating bogus packets and requests that clog the pipes.

Scaled attacks may be rare, but when they occur and a company is unprepared the losses can be devastating. Using DDoS protected web hosting is simply good business sense.

How Much Does DDoS Protected Web Hosting Cost?

The cost of protecting your website with DDoS mitigation can vary from one hosting company to the next. So, it's important to ask the right questions about what you are purchasing as it relates to the DDoS protection. Many hosting companies present you with gimmicks of unlimited storage space and more. When you read the fine print you discover it is not really unlimited. Or, when you begin to reach their limit you discover that it is not unlimited. Asking the right questions and reading the fine print is important. When comparing protection options, be sure that you know what you are comparing and the service that you are signing up for. Compare the specific features that you care about. It's highly unlikely that the $5 per month hosting package with everything unlimited probably does not have any kind of protection.

Small business owners will want a hosting package that not only provides the functionality and services they need but also adequate protection. Competitive hosting packages in a shared environment with a limited amount of DDoS protection included are going to start around $30/month. This type of a hosting package would be suitable for a small home-based business.

Businesses that rely heavily on internet traffic to their website should consider a virtual environment with more control over the web space. These services can be found for around $150/month with a limited amount of DDoS protection.

Usually enhancements are available for more comprehensive protection for another $150/month.

DDoSSupport.com offers all of the services and the full protection described in this report at competitive and affordable rates. For more information go to DDoSSupport.com or call 855-DDOSHelp, (855-336-7435.)