What Is A DDoS

A **distributed denial of service attack (DDoS)** occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. These systems are compromised by attackers using a variety of methods. Malware can carry DDoS attack mechanisms; one of the more well known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time.

This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack. A system may also be compromised with a trojan, allowing the attacker to download a zombie agent (or the trojan may contain one).

Attackers can also break into systems using automated tools that exploit flaws in programs that listen for connections from remote hosts. This scenario primarily concerns systems acting as servers on the web.

There are different kinds of DDoS attacks, but in general they can be difficult to manage and determine which connections are legitimate and which ones are not. Often times a more complicated firewall is put in place to filter out a lot of connections.

Sometimes other measure such as interfacing with another web server that can handle more connections than Apache may be taken as well. Unfortunately, after all these measures have been taken, sometimes all that can be done is to wait it out.